Etudes et observations des risques

2018-2

RISQUE ET PREDICTION

2018-2

Editorial

Depuis une trentaine d'années, les sapeurs-pompiers de France sont confrontés à une inexorable augmentation des demandes de secours. Pour structurer une réponse cohérente et optimale à la couverture des risques, les sapeurs-pompiers de Paris, et plus généralement les services d'incendie et de secours, ont donc besoin de concevoir de nouveaux systèmes qui caractérisent dans l'espace et dans le temps les vulnérabilités du territoire. Le projet de recherche DEMOCRITE (DEmonstrateur d'un MOteur de Couverture des RIsques sur un TErritoire), cofinancé par l'Agence Nationale de la Recherche (ANR-13-SECU-0007), constitue une étape majeure dans cette réflexion en agrégeant un vaste ensemble de données et en proposant dans une même application des outils de cartographie, de prédiction des risques et de représentation du territoire tout en modélisant finement certaines catégories d'interventions.

L'objectif du démonstrateur DEMOCRITE est d'intégrer des outils permettant d'analyser les risques (risques courants et deux risques majeurs) dans leurs deux dimensions : probabilités d'occurrence et conséquences, et d'offrir une analyse de la couverture de ces risques par les moyens disponibles. La construction de cet outil, coordonnée par le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) à partir des données de la Brigade des sapeurs-pompiers de Paris (BSPP) et pour répondre à ses besoins, a été élaborée par un consortium de huit partenaires dont le CERDACC (EA 3992), chacun intervenant dans son domaine de compétence.

Ce contrat de recherche a pris fin en septembre 2018 et dans la perspective de poursuivre la réflexion, il a été envisagé de travailler sur le thème de la prédiction, associé aux risques. En effet, pour améliorer la modélisation de la couverture des risques, les partenaires des disciplines scientifiques souhaitent orienter leurs recherches sur les conséquences de l'utilisation de modèles prédictifs toujours plus performants sur l'évaluation et la gestion du risque. C'est en ce sens qu'il convient d'apprécier la contribution à ce numéro de Christine et Emmanuel Lapébie, coordinateurs du projet et ingénieurs au CEA, se proposant de réfléchir sur la modélisation du risque, et sur l'utilité

d'améliorer les modèles de manière à diminuer l'aléa pour mieux prédire. L'idée de proposer un ensemble de contributions de nature à fournir un regard disciplinaire sur la prédiction au regard des principes juridiques applicables dans le domaine du risque, mais également de proposer une ouverture pluridisciplinaire, procède en quelque sorte d'une volonté d'explorer plus activement la robustesse des principes juridiques appliqués aux multiples facettes de la prédiction.

A commencer par le fondement même de la prédiction, à savoir le principe de prévention qui, à travers l'exemple du contrôle du juge sur les mesures de police administrative, développé par le Professeur Alexandre Ciaudo de l'Université de Bourgogne-Franche Comté, précise de quelle manière la prédiction caractérise le raisonnement du juge, une sorte de « retour aux sources », aboutissant, dans quelques hypothèses, à priver les individus des garanties liées à l'exercice des libertés en l'absence de proportionnalité de la mesure au regard de sa finalité. Le lien existant entre la prédiction et la prévention est, en effet, évident dès lors que prévenir suppose d'utiliser les données du passé, les appliquer à une situation présente pour éviter la réalisation future du risque.

L'utilisation d'algorithmes, plus simplement l'utilisation de modèles informatiques, faisant jouer et rejouer les scénarios du passé, permet de massifier les résultats obtenus et par conséquent de massifier les biais inhérents à la mise en œuvre du principe de prévention. En matière de risque industriel, la démarche n'est pas nouvelle et procède de l'analyse de risques des systèmes techniques, inféodés aux incertitudes aléatoires et épistémiques qui biaisent les résultats obtenus. Ces incertitudes sont connues et ne remettent pas en cause la démarche et la prise de décision qui s'ensuit. Cependant, c'est la modélisation du comportement humain qui est aujourd'hui visée, que ce soit en matière de couverture des risques par la modélisation de la rumeur, de la dispersion des foules, etc., ou dans le quotidien des individus lors de l'utilisation des services en ligne dans le but de modifier le référencement des services proposés en fonction de l'analyse comportementale des individus. Dès lors la question du libre arbitre, qui repose sur le discernement et l'expression de la manifestation de volonté est à nouveau posée et suppose de redéfinir juridiquement le consentement à l'ère

numérique de manière à limiter les effets de l'enfermement algorithmique. Ce principe occupe une place centrale dans l'architecture des textes, mais en réalité peu efficiente pour des motifs divers relevant des modalités techniques d'acquisition du consentement ; des modalités de mise à disposition des informations nécessaires au consentement ; des compétences techniques, de la dimension cognitive et affective de la personne qui consent sous contrainte avérée ou supposée ; de l'objet du consentement ; et enfin du consentement lui-même. Ériger le consentement en principe juridique dans ce contexte, procède de la volonté de lui conférer la simple faculté de s'opposer *a posteriori* au traitement, parce que la procédure visant à l'obtention du consentement a pour seule vocation d'informer la personne concernée du traitement de ses données en l'absence de démarche active de cette dernière liée à sa mise en pouvoir d'agir. En dépend la protection des droits de la personnalité « augmentés » à l'ère numérique découlant essentiellement du respect des normes visant à la protection des données à caractère personnel. Cette protection n'est pas aisée à mettre en œuvre en ce qu'elle requiert de décomposer l'ensemble des usages en la matière et de s'intéresser aux rapports de l'homme à la machine, pour comprendre à quel moment le respect des droits de la personnalité peut être remis en cause en raison de choix opérés par l'utilisateur lui-même sans qu'il soit en capacité d'en analyser la portée. A travers quelques exemples, Jeoffrey Sabbah, docteur en droit et enseignant contractuel à l'Université de Bourgogne-Franche Comté, illustre le processus. Un détour par les neurosciences, sous la plume d'Adrien Bouvel, maître de conférences HDR à l'Université de Strasbourg, met en perspective l'idée que la démarche du juriste doit s'ouvrir à d'autres disciplines pour « éduquer » d'une certaine manière notre cerveau à consentir valablement, à se mettre en situation d'apprenant en essayant d'agir sur les biais comportementaux et la relation de l'homme à la machine.

De la compréhension des phénomènes découle la prise de décision. Les modèles utilisés ne sont que des outils mis au service du décideur, avec des nuances selon que la décision relève de la sphère privée ou publique, et des enjeux inhérents aux disciplines concernées par la prise de décision. De manière à circonscrire plus finement le lien entre l'algorithme et la prise de décision, Paul Véron, maître de conférences en droit privé à l'Université de Nantes, s'intéresse à la décision médicale, tandis que Marcel Moritz, maître de

conférences HDR en droit public à l'Université de Lille, et sa doctorante Laurène Baudouin, traitent de la mesure de police prise dans le cadre de l'utilisation de drones. L'une des difficultés est de savoir qui dispose réellement du pouvoir de décision, notamment à partir de la définition des valeurs d'entrées qui alimentent les modèles et leur possible correction par des algorithmes auto-apprenants, autrement dit par l'utilisation de l'intelligence artificielle. La soumission au droit de ces algorithmes est envisagée comme pour mieux les apprivoiser. Certains principes sont évoqués tels que la loyauté, la neutralité, la non-discrimination ou la transparence. Aussi séduisants soient-ils en théorie, leur formulation et leur application à des cas concrets, sont loin d'emporter la conviction du juriste. C'est cette démonstration qui est portée par Colombe de Montety et Geneviève Bonhomme, juristes IP/IT et diplômées du Master Propriété intellectuelle et droit des affaires numériques (PIDAN) de l'Université Paris-Saclay. Dans la perspective de mieux réguler l'utilisation des algorithmes et par conséquent des places de marché, le principe de transparence semble désormais s'imposer à l'échelle européenne et celle des Etats membres … Pourtant, tel un objectif à atteindre, il permet d'imposer aux acteurs de mener une réflexion éthique conduisant à une utilisation raisonnée des algorithmes. C'est l'importance de ce principe qui est mis en perspective par Celia Zolynski, Professeure de l'École du droit de la Sorbonne de manière à limiter les actions en responsabilité. En tout état de cause, la corrélation algorithmique qui fonde l'analyse comportementale n'est pas synonyme de causalité, mais ne l'exclut pas. L'incertitude causale du rapport corrélatif présent dans l'usage des algorithmes prédictifs représente néanmoins un sujet d'inquiétudes pour le juriste. Mélis Aras, docteure en droit, et enseignante contractuelle à l'Université de Haute-Alsace, traite à ce titre des notions de causalité et de corrélation afin de montrer leur complémentarité.

Chers lecteurs, vous l'aurez compris, ce numéro de la revue *RISEO* a une vocation exploratoire dans l'objectif d'ouvrir le champ d'une réflexion plus ambitieuse encore, débarrassée des replis disciplinaires qui cantonnent la prédiction dans un cadre trop étroit pour en saisir tous les effets, positifs ou négatifs ! D'autres barrières de prévention et de protection issus d'autres champs disciplinaires, ont vocation à renforcer l'efficacité de la mise en œuvre

des principes juridiques révélés par la massification de la démarche prédictive. L'affaire est donc à suivre…

Bonne lecture !

Karine FAVRO, Maître de conférences en droit public, HDR, Université de Haute-Alsace, CERDACC (EA 3992).

Prévoir les risques, prédire les risques : utopie ou innovation ?

Christine LAPEBIE, Emmanuel LAPEBIE

Centre d'énergie atomique, DAM, GRAMAT, F-46500 Gramat, France

I) Projet ANR DEMOCRITE : chercheurs, pompiers et industriels unis pour l'analyse des risques

Le projet DEMOCRITE (ANR-13-SECU-0007-01) est un projet de recherche industrielle coordonné par le CEA. Il associe la Brigade de Sapeurs-Pompiers de Paris (BSPP), les sociétés ITLINK et SYSTEL, ainsi que des laboratoires de l'institut Pprime (P'), de l'IMT Mines Alès et du CERDACC ainsi qu'une équipe mixte INRIA/X. Le projet a commencé en mars 2014 et a duré 55 mois pour terminer en septembre 2018. Il a bénéficié d'une aide ANR de 995 426 € pour un coût global de l'ordre de 2,7 M€, avec un cofinancement SGDSN et DGA.

A) Urbanisme, grands évènements, menace terroriste… : Comment répondre aux futurs défis des services de secours ?

Les Services Départementaux d'Incendie et de Secours (SDIS), de même que la BSPP et le Bataillon de Marins-Pompiers de Marseille (BMPM) ont en charge l'élaboration de schémas d'analyse et de couverture des risques (SDACR) pour leurs territoires d'intervention et leur évolution périodique.

Ces dernières années ont vu une augmentation constante des interventions, le développement de nouvelles menaces (nuisances intentionnelles à distinguer des risques qui sont des nuisances accidentelles) et un besoin accru de gestion des grands événements, cibles potentielles d'attaques (coupe du monde 2016, J.O. 2024, etc.) sur des territoires d'une grande complexité, en particulier en milieu urbain.

Au démarrage du projet, le besoin de développer des outils d'analyse et de couverture des risques était devenu pressant. Ces outils devaient pouvoir

s'intégrer au socle commun SIG mis en place à la Préfecture de Police de Paris, dans le but de répondre, au mieux, aux attentes des populations et de respecter les engagements de la BSPP.

B) DEMOCRITE propose une approche pluridisciplinaire basée sur une plateforme cartographique d'analyse et de couverture de risques.

Pour répondre à ces objectifs, l'approche pluridisciplinaire adoptée dans DEMOCRITE a permis de tirer le meilleur parti des compétences de chacun :

- les opérationnels (BSPP) ont apporté leur connaissance des besoins et du territoire ainsi que leur retour d'expérience,
- les chercheurs (CEA, Pprime, IMT Mines Alès, INRIA/X et CERDACC) ont développé des approches innovantes pour traiter les problèmes scientifiques et juridiques,
- les industriels (ITLINK et SYSTEL) ont intégré ces approches, tout en contribuant également aux recherches scientifiques.

L'analyse préliminaire du besoin avait identifié les composants nécessaires pour une plateforme logicielle d'analyse et de couverture de risques :

- des données géographiques maîtrisées,
- la cartographie des risques courants dans leurs deux dimensions : probabilité d'occurrence (selon les interventions passées ou par analyse prédictive) et conséquences potentielles (vulnérabilités humaine et fonctionnelle),
- des premiers modèles rapides pour certains risques majeurs (explosion en milieu urbain et incendie sans intervention des secours),

Les partenaires ont ajouté, durant le projet, la cartographie de disponibilité des moyens à un instant donné (couverture des risques) et la cartographie des risques résiduels.

C) Données et algorithmes, au cœur de DEMOCRITE.

DEMOCRITE repose d'abord sur des données : la BSPP a communiqué aux partenaires du consortium plus de 700 couches de données géographiques vectorielles concernant son territoire d'intervention, ainsi que six années de

données d'interventions géolocalisées (RETEX). DEMOCRITE intègre également des modèles rapides de simulation pour deux risques majeurs, et vise à incorporer, à terme, l'ensemble des modèles nécessaires pour procéder à une analyse quantitative des risques.

Les modèles de simulations appartiennent à trois grandes catégories :

- les modèles empiriques, qui ne reposent pas sur une mise en équation des phénomènes mais sur la restitution par une formulation mathématique de résultats déjà connus (interpolation), en fonction de variables explicatives « logiques »,
- les modèles analytiques, qui nécessitent une mise en équation des phénomènes et l'élaboration d'hypothèses simplificatrices de manière à pouvoir résoudre ces équations de manière rapide,
- les modèles numériques, fréquemment associés à une discrétisation temporelle et une discrétisation spatiale 2D ou 3D, qui résolvent les équations descriptives du phénomène avec un minimum d'hypothèses simplificatrices, au détriment d'une puissance de calcul requise importante, d'une durée de simulation non négligeable et d'une utilisation par des experts.

DEMOCRITE privilégie les modèles de la deuxième catégorie, qui associent un fonctionnement rapide nécessaire pour les situations d'urgence ou l'étude de scénarios paramétriques et des fondements physiques qui doivent éviter les résultats aberrants.

Par ailleurs, une étude préliminaire menée dans le projet concerne l'analyse prédictive des interventions, l'objectif étant de déterminer d'éventuelles corrélations entre les caractéristiques du territoire et l'occurrence de certains types d'interventions à certains endroits et à certains moments. Ces corrélations forment un ensemble de modèles empiriques propres à étudier le changement du nombre et de la nature des interventions en fonction de modifications possibles du territoire, afin d'optimiser la couverture des risques auxquels les citoyens peuvent être confrontés.

Données, modèles de simulation et modèles empiriques tirés d'analyses prédictives présentent chacun des incertitudes de différentes natures, qui doivent être prises en compte lors des processus de prise de décision compte-tenu de la gravité des enjeux et des impacts possibles d'une décision erronée. Les deux sections qui suivent abordent quelques réflexions sur les incertitudes dans les résultats de simulation (section 2) et sur les problèmes posés par l'analyse prédictive (section 3).

Faute de place, le présent article traitera peu des données proprement dites, qui servent pourtant de base à la fois aux modèles de simulation et aux analyses prédictives. Pour DEMOCRITE, nous avons identifié comme « qualités » requises pour les données les éléments suivant : disponibilité, géolocalisation, pertinence, complétude, accessibilité, structuration, fiabilité, mise à jour…

La prise en compte de ces critères n'en est qu'à ses débuts en France, mais les initiatives se multiplient et se structurent : Conseil national de l'information géographique (CNIG), site internet data.gouv.fr, rapport sur les données géographiques souveraines[1]…

II) Prévoir les risques : incertitudes sur les résultats de simulation

Pour de nombreux risques, l'approche scientifique consiste à établir des modèles de simulation représentatifs de la physique des phénomènes sous-jacents (dans DEMOCRITE, deux modèles de simulation sont implémentés, pour le calcul des conséquences d'une explosion d'une part, et pour le calcul des conséquences d'un incendie sans intervention des secours d'autre part).

Un modèle de simulation est constitué de quatre éléments :

- des variables d'entrée (variables explicatives),
- des relations ou fonctions mathématiques reliant ces variables d'entrée et celles de sortie (le modèle proprement dit),
- des paramètres fixes,

[1] V. FAURE-MUNTIAN, *Les données géographiques souveraines*, rapport au gouvernement remis par la députée de la Loire, Juillet 2018.

- des variables de sortie (variables expliquées).

À chacun de ces éléments, nous étudierons dans les paragraphes qui suivent les sources d'incertitude, en leur associant un exemple tiré du projet DEMOCRITE.

A) Variables d'entrée (variables explicatives)

Si on considère que le modèle reproduit bien la réalité, la principale source d'incertitude est la variation des variables d'entrée du modèle. En effet, les variables d'entrée sont rarement connues de manière déterministe, c'est-à-dire, sans aucune incertitude, et sont d'autre part sujettes à des erreurs humaines lors de leur saisie. Il est alors important de connaître l'influence de l'imprécision de ces variables d'entrées sur les variables de sortie du modèle, c'est-à-dire étudier la propagation d'incertitude :

1. en déterminant l'incertitude sur la connaissance des variables d'entrée et en la traduisant sous forme de loi de probabilité,
2. en propageant cette incertitude sur les sorties du modèle pour en connaitre les distributions.

Dans DEMOCRITE, les données de RETEX sont localisées au centre des tronçons routiers (représentation vectorielle des rues dans le système d'information géographique) et non pas sur le lieu même de l'intervention. Les données sont ensuite projetées sur le carroyage opérationnel BSPP (carreaux de 200 m x 200 m). Ces imprécisions peuvent avoir des conséquences sur le calcul de la couverture des risques.

B) Fonctions mathématiques constitutives du modèle

Un modèle, aussi complexe soit-il, n'est qu'une représentation simplifiée de la réalité. Les résultats du modèle diffèreront donc des résultats « réels », et les différences peuvent être notables.

Dans DEMOCRITE, le modèle d'explosion en milieu urbain FLASH vise justement à pallier les déficiences jugées inacceptables des modèles « classiques » qui, pour une explosion en champ libre, se traduisent par des cercles concentriques d'iso-dommages aux personnes et aux biens. Quand on compare les résultats calculés par FLASH à des expériences, il existe néanmoins toujours un écart car le modèle se base sur des hypothèses simplificatrices.

C) Paramètres fixes

Le modèle est en partie constitué de paramètres fixes (par exemple les coefficients d'une fonction mathématique ou le paramétrage des algorithmes de résolution d'équations). Ces coefficients doivent être calibrés à partir de « mesures » pour réduire au mieux l'erreur de prédiction du modèle.

Dans DEMOCRITE, c'est le cas en particulier du modèle de propagation d'incendie à l'échelle urbaine. Les paramètres de ce modèle ont pu être identifiés pour reproduire au mieux un incendie majeur dans une ville japonaise (Kobé) notablement différente des métropoles européennes, pour lesquelles aucun incendie récent de grande ampleur n'a été à déplorer (les incendies historiques de Londres, New York, etc. étant trop sommairement décrits pour pouvoir en inférer des paramètres). Cela constitue un biais dans la modélisation adoptée.

D) Variables de sortie (variables expliquées)

Une fois le modèle calibré et validé, on pourra l'utiliser pour prédire. Ces prédictions pourront être utilisées pour déterminer les variables d'entrée qui constituent les compromis optimaux entre les différentes sorties du modèle.

Dans DEMOCRITE on pourra ainsi, par exemple, tenter d'optimiser la position des moyens d'intervention pour satisfaire une forte demande de secours tout en limitant l'utilisation des ressources nécessaires.

Si une étude de propagation d'incertitude peut être menée, elle permettra de faire apparaître comme aide à la décision non plus un résultat déterministe,

mais un résultat prenant en compte les incertitudes sur les variables de sortie. De telles démarches ont fait l'objet de plusieurs recherches, en particulier dans le domaine de la dispersion atmosphérique[2].

III) Prédire les risques : incertitudes sur les analyses prédictives

L'article Wikipedia éponyme indique que « *L'analyse (ou logique) prédictive englobe une variété de techniques issues des statistiques, d'extraction de connaissances à partir de données et de la théorie des jeux qui analysent des faits présents et passés pour faire des hypothèses prédictives sur des événements futurs* ». D'abord appliquées aux risques financiers et bancaires (par exemple le *FICO score* pour les risques de non remboursement de crédits[3]), ces techniques ont connu un essor récent dans de nombreux autres domaines.

Les approches utilisées pour l'extraction des connaissances (apprentissage profond ou *deep learning*) ont été pour la plupart élaborées il y a plusieurs dizaines d'années[4], mais le développement exponentiel des puissances de calcul (loi de Moore) permet à présent de les appliquer à des volumes de données suffisamment importants pour des applications réalistes.

A) « Nous vivons de et par l'anticipation. […] Elle est constitutive de notre mode de vie, une société toute entière fondée sur la prévision et la réduction du risque » - Bruno Jarrosson, *Briser la dictature du temps*, cité par François Delivré dans *Question de temps*.

Au risque de paraître iconoclaste, l'analyse prédictive actuelle n'est que l'héritière des techniques divinatoires[5] utilisées depuis la nuit des temps par les

[2] Par exemple la thèse de S. PAGNON « *Stratégies de modélisation des conséquences d'une dispersion atmosphérique de gaz toxique ou inflammable en situation d'urgence au regard de l'incertitude sur les données d'entrée* », soutenue en 2012 (https://tel.archives-ouvertes.fr/tel-00844130); ou la thèse de N. BAO TRAN LE en cours à l'IRSN, « *Quantification d'incertitude par réduction de modèle de dispersion atmosphérique* ».

[3] https://www.investopedia.com/terms/f/ficoscore.asp

[4] Se référer par exemple à la bibliographie de la thèse de C. LAPEBIE « *Implémentation et optimisation de stratégies de décision* », soutenue en 1995 : la formalisation de l'utilisation des réseaux neuronaux, du recuit simulé, des algorithmes génétiques et des techniques associées date du milieu des années 1980.

[5] Le terme « prédire » plutôt que « prévoir » a d'ailleurs une connotation plus irrationnelle.

êtres humains. L'article Wikipedia « Art Divinatoire » offre un aperçu édifiant des multiples approches élaborées au cours des siècles pour répondre à notre angoisse existentielle : « de quoi demain sera-t-il fait ? ».

La majorité de ces techniques divinatoires repose sur le postulat non formulé d'une corrélation (ou plus rarement d'une causalité)[6] entre l'objet de l'art divinatoire (lien avec une entité omnisciente, caractéristiques d'entrailles d'animaux, position des planètes, images formées par des feuilles de thé, …) et le destin du sujet étudié. Historiquement, ce sujet d'étude a tout d'abord été collectif : un pays ou un peuple dans son ensemble, puis les dirigeants ou chefs de guerre dont le destin était par nature corrélé à celui d'un groupe plus vaste, et enfin chaque individu potentiellement intéressé. En parallèle à ce passage de l'intérêt global à l'intérêt particulier, les réponses attendues ont évolué : l'occurrence d'événements majeurs pouvant changer le devenir d'une population entière (invasion, fin du monde…), des événements importants (naissance, décès, victoire ou défaite miliaire), pour aboutir à des questions d'ordre individuel (avenir professionnel, financier, social, amoureux …).

Les techniques modernes d'analyse prédictive cherchent également à établir la modélisation empirique d'un lien possible entre des variables d'entrées connues (variables explicatives) et des variables de sortie à prédire (variables expliquées). Elles ne recherchent donc pas un lien de causalité (car si la causalité était explicite il serait possible de bâtir directement un modèle analytique), mais bien une simple corrélation. On ne s'intéresse donc pas à la phénoménologie physique sous-jacente (ni même à des variables explicatives « logiquement » pertinentes, contrairement aux modèles empiriques de simulation précédemment abordés) mais simplement à l'établissement d'un modèle mathématique plus ou moins complexe.

[6] Ce lien non explicite n'est autre qu'un « modèle empirique » du phénomène étudié. Gardons-nous de tout anachronisme : la pensée magique était par le passé le fonctionnement « scientifique » nominal qui guidait l'appréhension de l'univers, et la notion de science moderne est récente (cf. travaux sur l'épistémologie). Aux portes de la Renaissance, les universités enseignaient le latin et le grec, la théologie, la médecine, mais aussi l'alchimie et l'astrologie !

B) « Deux augures ne peuvent se regarder sans rire » - Cicéron, *De divinatione*, II, 24

Quelle différence alors entre les techniques divinatoires et l'analyse prédictive moderne ?

La différence principale repose sur le mode d'élaboration des liens entre variables explicatives et variables expliquées. Les arts divinatoires présupposent un lien entre ces deux types de variables, sans risquer de confrontation avec une validation statistique – délicate au demeurant (à l'exception notable de travaux portant sur certains aspects de l'astrologie[7]). L'analyse prédictive quant à elle déduit des corrélations statistiquement valides à partir des données elles-mêmes, chiffre la qualité des corrélations observées, et ne retient que les plus pertinentes au regard de l'emploi envisagé.

Plusieurs écueils persistent (outre la qualité des données utilisées) et ne sont pas forcément pris en compte dans les travaux récents d'analyse prédictive :

- le biais du « *big data* »,
- la tentation du « *cum hoc ergo propter hoc* » (avec ceci, donc à cause de ceci),
- l'individualisation des prédictions.

Pour le premier écueil, il faut remarquer qu'une démarche scientifique classique part d'un postulat initial et développe une démarche de pensée visant à valider ou invalider ce postulat[8]. *A contrario*, l'analyse prédictive vise à « faire parler » les données elles-mêmes, avec le risque de faire apparaître des coïncidences plutôt que des corrélations. Les tests de vraisemblance statistique renseignent sur la probabilité qu'une corrélation observée soit due au hasard (on considère généralement qu'un résultat inférieur à 5% est « significatif »). Toutefois, lorsque l'on teste de manière automatique des milliers – voire des millions – de corrélations potentielles, il y en aura forcément qui apparaîtront

[7] https://fr.wikipedia.org/wiki/Étude_statistique_de_l'astrologie

[8] Claude BERNARD écrivait dans *Introduction à l'étude de la médecine expérimentale* «*Un fait n'est rien par lui-même, il ne vaut que par l'idée qui s'y rattache ou la preuve qu'il fournit* »

significatives à des seuils assez faibles… par pur hasard et sans pour autant avoir une quelconque capacité prédictive !

Le site « *spurious correlations* » (corrélations fallacieuses) (http://www.tylervigen.com/spurious-correlations) de Tyler Vigen recense ainsi de nombreuses coïncidences entre des séries temporelles de données aux USA, par exemple entre le nombre de suicides par pendaison, strangulation et suffocation et les dépenses dans le domaine des sciences, de l'espace et des technologies (coefficient de corrélation 0,998, sachant qu'un coefficient de 1 indique une corrélation parfaite !).

Le deuxième écueil est lié à une confusion fréquente entre coïncidence, corrélation et causalité. L'expression latine déjà citée *cum hoc ergo propter hoc* illustre notre tendance naturelle à confondre ces termes. Pourtant, si deux variables A et B sont corrélées, on peut avoir une non-causalité (coïncidence), une causalité directe (A $\Rightarrow$ B) ou inverse (B $\Rightarrow$ A), voire bidirectionnelle (A $\Rightarrow$ B et B $\Rightarrow$ A), une causalité liée à une troisième variable non étudiée C[9] (C $\Rightarrow$ A et C $\Rightarrow$ B, ou A $\Rightarrow$ C et C $\Rightarrow$ B), ou encore un schéma beaucoup plus complexe.

Une étude sur de nombreux pays montre par exemple qu'il a une corrélation positive entre la consommation de viande et l'espérance de vie, qui peut s'expliquer par une troisième variable liée à la richesse du pays (par exemple le PIB par habitant). En effet, a) il y a corrélation positive entre le PIB par habitant et l'espérance de vie ; b) il y a corrélation positive entre le PIB par habitant et la consommation de viande et c) il y a corrélation négative entre la consommation de viande et l'occurrence de certaines maladies. La corrélation négative (causalité) est faible par rapport aux deux corrélations positives, et est plus que compensée par une médecine plus évoluée (dépistage et traitement) dans les pays à PIB par habitant élevé, d'où la corrélation positive globale…

Enfin, le troisième écueil est lié à « l'oubli » du mode de détermination des corrélations, à savoir l'agrégation d'un grand nombre d'items (événements,

[9] Appelées parfois « variables de confusion ». Il existe ainsi un lien avéré entre le nombre de fautes d'orthographes lors de dictées et la pointure des élèves de primaire (corrélation négative). La variable de confusion non explicitée est l'âge, dont le lien de causalité avec la taille des pieds et la maîtrise de l'orthographe est parfaitement explicable… mais ne peut pas être étendu à l'âge adulte !

personnes, etc.) indispensable pour obtenir une corrélation statistique fiable. La tentation est grande d'appliquer alors ces corrélations à un individu ou à un groupe d'individus donné (qui de plus ne répondent pas nécessairement à la même distribution statistique que l'ensemble des données utilisées pour déterminer les corrélations initiales). Si l'application de techniques d'analyse prédictive est parfaitement adaptée (et efficace) pour déterminer des points chauds de criminalité urbaine (*predictive policing*), est-elle encore légitime pour juger si un individu donné présente un risque particulier ?

Aux États-Unis, des logiciels[10,11] (*risk assessment tools*) sont déjà utilisés pour prédire le risque de récidive lors d'une demande de libération conditionnelle, réduisant à néant la capacité individuelle des individus à maîtriser leur destin (repentir, libre arbitre, …), et postulant une forme de « déterminisme » (tout individu agit en moyenne comme la masse) d'ailleurs contradictoire avec l'aspect intrinsèquement stochastique des phénomènes. Par ailleurs, il a été prouvé que certains de ces algorithmes, loin d'être objectifs, reproduisaient les inégalités raciales et sociales. La justice prédictive illustrée dans le film *Minority Report*, tiré du roman de Philip K. Dick, n'est plus loin : certains sites[12] proposent d'anticiper les décisions de justice en établissant les probabilités de recevabilité des arguments utilisés et en évaluant même le montant d'éventuelles indemnités[13], et la justice française semble s'engager dans cette voie[14]…

C) *Algorithms evolve, push us aside and render us obsolete* (Les algorithmes évoluent, nous poussent sur le bas-côté et nous rendent obsolètes) – Muse, Algorithms

[10] B. BUTLER, *Predictive Analytics in Health Care and Criminal Justice: Three Case Studies*, June 2015.
[11] L. FERNANDEZ RODRIGUEZ, *Un algorithme peut-il prédire le risque de récidive des détenus ?*, août 2017, publié sur : https://usbeketrica.com/article/un-algorithme-peut-il-predire-le-risque-de-recidive-des-detenus .
[12] Par exemple Predictice en France, (https://predictice.com/) dont la page d'accueil annonce « *Au cœur de la justice. Analysez des millions de décisions de justice en 1 seconde* ».
[13] A. BUDRY CARBÓ, *La justice prédictive se prépare à envahir le monde juridique*, mai 2017, publié en ligne : https://www.letemps.ch/economie/justice-predictive-se-prepare-envahir-monde-juridique .
[14] L. GARRIGUE, *Quand la justice se robotise ! Rencontre avec Antoine Garapon*, in Sciences Humaines, décembre 2018.

Dans de nombreux domaines, les algorithmes ne se contentent plus de fournir une aide à la décision, laissant le jugement final à un être humain doté d'émotions et d'empathie. Des systèmes autonomes aptes à évaluer des risques et à prendre des décisions (robots dotés d'une intelligence artificielle, véhicules autonomes …) sont en phase de test ou parfois déjà commercialisés, prenant de court les multiples questions éthiques et juridiques qui ne manquent pas de se poser[15].

La prise de décision (humaine à l'origine, telle que celle liée à l'évaluation des risques) impliquant potentiellement d'infliger des blessures ou de tuer (de manière non intentionnelle, le cas des robots de combat étant ici exclu de l'analyse) un ou plusieurs êtres humains a conduit à l'élaboration de nombreuses expériences de pensée, dont la plus connue est peut-être le dilemme du tramway, dont la version de base (Tuer ou laisser mourir, ou *Kill or let die*) s'exprime par : un piéton assiste à la course incontrôlable d'un tramway dont les freins ont lâché, et se trouve confronté à l'alternative suivante : soit il ne fait rien et le tramway continue sur sa voie normale où travaillent 5 ouvriers (et les tue tous – *Let die option*), soit il actionne un aiguillage et oriente le tramway vers une voie de garage où se trouve un seul individu (qui va donc mourir suite à cette décision – *Kill option*).

Une abondante littérature est consacrée à ce dilemme (en éthique, sciences cognitives, etc.) et à ses multiples variantes[16], pour aboutir récemment à des critiques fondamentales sur la différence entre « ce que l'on dit que l'on ferait » et « ce que l'on ferait effectivement », remettant en cause les expériences de pensées « trop éloignées de situations réalistes »… Cependant, c'est exactement à ce type de choix que seront confrontés les véhicules autonomes, et les constructeurs réfléchissent à l'implémentation « *d'algorithmes de la mort* »[17] en prévision de ces décisions. Une voiture pourrait par exemple décider de sacrifier la vie de son conducteur pour sauver plusieurs piétons… Peut-être trouvera-t-on dans ces voitures un réglage

[15] Voir par exemple *le Livre blanc sur la justice prédictive*, publié en novembre 2018 par l'école de droit de SciencesPo (J.-V. HUSS, L. LEGRAND et T. SENTIS).

[16] Il est possible de tester nos propres décisions sur des dilemmes du même type grâce au site suivant : http://moralmachine.mit.edu/ .

[17] A. DEBROISE, *Voiture autonome : l'algorithme de la mort*, Science & Vie, 2016 mis à jour en 2018.

« d'altruisme », comme on en trouve déjà pour de multiples paramètres de conduite.

Que nous le voulions ou non, l'énorme pression technologique, commerciale et politique[18] conduira dans les années à venir à laisser à des machines une autonomie de décision, y compris pour l'analyse et la gestion des risques de toute nature. Le développement des systèmes autonomes ayant connu une accélération inattendue, des éléments de réponse peuvent être recherchés… dans les romans d'anticipation. Isaac Asimov, dans ses écrits sur les robots intelligents, a le premier eu l'idée d'un nombre limité de lois à mettre en place « en dur » au sein des intelligences artificielles. Les trois lois de la robotique, complétées plus tardivement par la « loi 0 » qui place la sécurité de l'humanité avant celle d'un individu, s'énoncent ainsi :

- Loi 1 : Un robot ne peut porter atteinte à un être humain, ni, en restant passif, permettre qu'un être humain soit exposé au danger ;
- Loi 2: Un robot doit obéir aux ordres qui lui sont donnés par un être humain, sauf si de tels ordres entrent en conflit avec la première loi ;
- Loi 3 : Un robot doit protéger son existence tant que cette protection n'entre pas en conflit avec la première ou la deuxième loi.

Malheureusement, ces trois lois fondamentales peuvent être contournées de multiples manières, comme le montrent d'ailleurs les romans d'Asimov… et le problème reste donc entier.

Il faut bien sûr distinguer les dangers réels liés aux algorithmes des dangers fantasmés par certains, mais nous ne partageons pas sur ce point la sérénité de certains chercheurs[19]…

IV) En conclusion : vers un « droit des algorithmes » et une « éthique des intelligences artificielles » ?

Concernant les algorithmes liés à la prévision/prédiction des risques (modèles de simulation ou analyse prédictive), et sans aller jusqu'au

[18] C. VILLANI, *Donner un sens à l'intelligence artificielle – pour une stratégie nationale et européenne*, rapport de la mission parlementaire menée du 8 septembre 2017 au 8 mars 2018.

[19] Entrevue avec Serge ABITEBOUL (chercheur à l'INRIA) dans Face au risque n°547, intitulée « Les algorithmes sont source d'inquiétude, mais peuvent être maîtrisés ».

fonctionnement des machines autonomes[20], nous pouvons noter qu'une plateforme d'aide à la décision telle que DEMOCRITE entraine déjà des questionnements sur le cadre juridique associé. Ces questionnements sont principalement de trois ordres :

- l'utilisation des données (pour la création du modèle ou lors de son utilisation),
- la responsabilité vis-à-vis d'une prise de décision liée aux prédictions faites par un tel outil,
- les biais liés à l'utilisation de données statistiques pour en tirer des lois prédictives.

Pour le premier point, en aucun cas une donnée personnelle ne peut être utilisée si elle n'est pas soit rendue anonyme, soit accompagnée d'une autorisation d'utilisation. Mais l'agglomération et le croisement de données anonymes ou libres d'utilisation peut conduire à la constitution d'une donnée individualisée dont l'utilisation n'a pas été autorisée.

Pour le deuxième point, *quid* de la responsabilité du décisionnaire (qui est rarement le concepteur de l'outil) dans le cas d'une mauvaise prédiction qui entrainerait un préjudice ? La responsabilité du concepteur de l'algorithme peut-elle être engagée ? Une première réponse issue des groupes de travail DEMOCRITE est que la chaîne de responsabilité est liée à la chaîne de validation de l'outil et à son cadre d'utilisation. De plus, un outil de prédiction doit toujours être présenté comme un outil d'aide à la décision et non comme un outil de décision, sachant de plus qu'un modèle, aussi performant soit-il, n'est qu'une vision approchée de la réalité.

Pour le troisième point enfin, il faut se questionner sur le caractère discriminatoire ou politiquement incorrect que peut fournir le résultat d'un outil de prédiction basé sur des corrélations statistiques (qui peuvent, nous l'avons vu, n'être parfois que des coïncidences). Que faire si les résultats de prédiction, couplés à une connaissance locale de la population, permettent de cibler une minorité comme étant plus à risque qu'une autre ?

[20] On peut néanmoins noter les vifs débats sur l'opportunité de créer ou non une « personnalité juridique » pour les robots, entre « personne physique » et « personne morale »…

Il est donc urgent que les aspects juridiques liés à l'utilisation d'algorithmes soient abordés, en y intégrant les aspects éthiques indispensables pour vérifier l'acceptabilité sociétale de certaines innovations. La partie 5 « Quelle éthique pour l'IA » du rapport de Cédric Villani sur l'intelligence artificielle, déjà cité, ouvre quelques pistes de réflexion[21], qu'il faut sans attendre développer et structurer, sans réserver le débat à certains spécialistes.

Remerciements

Les auteurs remercient les membres du groupe de travail « Analyse Prédictive » organisé février 2018 pour préparer les suites du projet DEMOCRITE. Certaines des idées développées dans cet article sont directement issues de leurs réflexions.

[21] Notamment sur l'explicabilité des systèmes à base d'apprentissage (analyse prédictive), dont les auteurs reconnaissent qu'elle « constitue […] un véritable défi scientifique »…

La prédiction administrative de l'atteinte à l'ordre public

Alexandre CIAUDO

Professeur agrégé de droit public à l'Université de Bourgogne-Franche-Comté (CRJFC), Avocat à la Cour

Envisager les contours d'une notion juridique de prédiction peut ressortir tant de la gageure que de l'authentique antinomie. Une telle étude, spécialement appliquée au domaine du droit administratif, et plus précisément à celui de la police administrative, constitue pourtant un véritable retour aux sources. Dans son sens le plus courant, la prédiction renvoie à l'action d'annoncer la survenance d'un événement futur par une inspiration surnaturelle ou divine. Elle s'assimile alors à la prophétie et repose sur la croyance de son destinataire en une écriture de son propre destin par une autorité ou puissance supérieure à laquelle il ne peut échapper. De l'Oracle de Delphes à Nostradamus, de nombreuses prédictions auraient été révélées à des individus sur l'avenir, l'obscurité et la généralité de leur formulation permettant au demeurant de certifier leur réalisation par une simple interprétation des paroles du devin.

La prédiction peut au contraire s'analyser comme le résultat d'un authentique travail scientifique. Il s'agit alors d'annoncer la survenance d'un événement à venir par la mise en œuvre d'un raisonnement, d'une induction ou d'un calcul. En ce sens, les astronomes, à l'opposé des astrologues, sont capables de prédire les éclipses en anticipant le déplacement des astres. A cet égard, une assertion de Bergson dans sa thèse de doctorat publiée en 1889 invite à la réflexion : « *Les raisons qui font que la prédiction d'un phénomène astronomique est possible sont précisément les mêmes qui nous empêchent de déterminer à l'avance un fait émanant de l'activité libre* »[22]. A suivre l'éminent philosophe, l'activité sociale ne pourrait être prédite à peine d'en restreindre le

[22] H. BERGSON, *Essai sur les données immédiates de la conscience*, thèse, Félix Alcan, 1889, p. 150.

libre exercice. Si ce propos exige une relativisation lorsque l'auteur de la prédiction analyse des faits sociaux et suppose leur évolution prévisible dans le temps, il s'avère parfaitement exact quand la prédiction se concrétise par une intervention projetée dans le but d'empêcher la survenance d'un événement probable.

Ainsi, par son travail d'interprétation des textes et de la jurisprudence, la doctrine procède précisément à des prédictions des conséquences possibles de certaines décisions des autorités normatives[23]. En ce sens et à titre d'illustration, dans sa première note d'arrêt, rédigée sous l'arrêt Cadot rendu également en 1889, Maurice Hauriou annonçait « qu'à l'avenir », et à raison de la disparition de la théorie du ministre-juge, les justiciables devraient saisir directement le Conseil d'Etat de leurs recours contentieux dans le délai de recours contentieux[24]. L'analyse d'une règle procédurale nouvelle laissait ainsi présager une évolution des comportements des usagers du service public de la justice.

La prédiction, alors entendue comme une annonce d'événements futurs par l'analyse de leurs causes, constitue une méthode mise en œuvre de manière courante par les acteurs du droit administratif, et notamment par les autorités de police administrative. On sait à ce titre que les mesures de police sont édictées dans le but spécifique de préserver l'ordre public et non dans un objectif de simple satisfaction de l'intérêt général[25]. Le rôle de l'autorité de police consiste à anticiper la survenance d'une atteinte à l'ordre public en édictant une mesure de nature à l'empêcher. Pour reprendre l'expression du sociologue américain Robert King Merton, la fonction de la police administrative pourrait être comprise comme une mise en œuvre systématique de prophéties autodestructrices.

A rebours de la prophétie autoréalisatrice qui correspond à un énoncé modificateur et provocateur des comportements qu'il annonce, la prophétie autodestructrice consiste en une prédiction qui détruit les possibilités de sa réalisation. Néanmoins, pour l'autorité de police administrative, la seule

[23] N. MOLFESSIS, « Les prédictions doctrinales », *Mélanges François Terré*, PUF-Dalloz, 1999, p. 141.
[24] M. HAURIOU, note sous CE, 13 décembre 1889, Cadot, *S*. 1892 III, p. 17, *Notes d'arrêts*, La mémoire du droit, 2000, t. 2, p. 441.
[25] CE, 10 avril 1992, Aykan, n° 75006, Rec. 153, *RFDA* 1993, p. 541, concl. M. Denis-Linton.

annonce d'un évènement à venir ne suffit pas à empêcher sa réalisation. L'anticipation de l'avenir exige au contraire une intervention de l'administration de nature à empêcher sa matérialisation future.

Alors que la police judiciaire prend acte de la commission passée d'une violation de la loi pénale et vise à sa répression, la police administrative a pour objet de prédire une atteinte future à l'ordre public et de la prévenir, c'est-à-dire de se projeter au-devant de cette atteinte en empêchant son accomplissement. Edicter une mesure de police administrative revient alors bien à prédire pour prévenir.

Lorsque le Président Emile Loubet a, le 10 mars 1899, institué par décret un certificat de capacité pour la conduite automobile, il a nécessairement prédit que, eu égard aux dangers pour la population résultant de cette activité en plein essor, l'absence de régulation de l'utilisation des véhicules automobiles conduirait à des drames humains. Il a donc « en dehors de toute délégation législative et en vertu de ses pouvoirs propres » pu mettre en œuvre cette mesure de police administrative en restreignant le droit de propriété et la liberté d'aller et venir des individus afin de protéger la sécurité publique[26]. Une telle prédiction ne relevait ni de la divination ni de l'étude des corps célestes, mais du bon sens.

Toutefois, l'édiction de mesures de police administrative peut parfois résulter de prédictions administratives plus discutables, notamment lorsqu'il s'agit d'interdire une réunion publique, un spectacle, ou une manifestation au nom de l'atteinte probable à l'ordre public qui pourrait résulter de son déroulement, voire de proscrire le port d'un vêtement sur la voie publique en raison des réactions qu'il serait susceptible de générer. Plutôt que de jeter l'opprobre sur les supposées capacités divinatoires de l'administration, et sur une complicité passive de son juge, il peut s'avérer plus pertinent de s'intéresser aux modalités concrètes du contrôle du juge sur les prédictions de l'autorité de police administrative, à travers l'appréciation concrète de la nécessité des mesures de police (sans qu'il besoin à ce stade de s'intéresser à

[26] CE, 8 août 1919, Labonne, Rec., p. 737.

l'adaptation et à la proportionnalité[27]). On constate alors qu'en matière de police administrative, le juge administratif exige de l'autorité de police qu'elle justifie des éléments lui ayant permis de formuler sa prédiction de l'atteinte à l'ordre public, puis exerce un contrôle sur le contenu de la prédiction.

I) La justification des données de la prédiction

Avant que, dans le but d'assurer l'ordre public, l'autorité de police administrative ne décide des mesures et n'entreprenne des actions propres à prévenir les risques d'atteinte à l'ordre public[28], elle devra démontrer la matérialité d'un désordre à prévenir[29]. Ainsi, afin d'édicter une mesure de police administrative, l'autorité administrative se fonde sur un certain nombre d'informations dont elle dispose qui la conduiront à supposer la commission future d'une atteinte à l'ordre public. La nécessité même de la mesure de police dépend donc de la réunion d'éléments concordants qui auront permis à l'autorité compétente d'élaborer sa prédiction.

Le rôle du juge administratif saisi de la légalité de la mesure de police sera alors avant toute chose d'analyser les données de la prédiction administrative. En d'autres termes, le juge appréciera la nécessité de l'édiction de la mesure de police en fonction des éléments mis en avant par l'autorité administrative sur la probabilité de la survenance de l'atteinte à l'ordre public.

L'étude de cette partie du contrôle juridictionnel se heurte régulièrement au laconisme rédactionnel des arrêts du Conseil d'Etat qui se contente dans certaines décisions de l'utilisation de périphrases ne permettant pas de déterminer les éléments précis avancés au soutien de la prédiction de l'autorité administrative : « il ne ressort pas de l'instruction »[30], « il ne ressort pas des pièces du dossier »[31]. L'emploi de ces locutions stéréotypées révèle certes que le Conseil d'Etat a examiné les données de fait et en a tenu compte, mais

[27] V. not. Sur cette trilogie C. ROULHAC, « La mutation du contrôle des mesures de police administrative. Retour sur l'appropriation du « triple test de proportionnalité » par le juge administratif », *RFDA* 2018, p. 343.
[28] R. CHAPUS, *Droit administratif général tome 1*, 15e éd., Montchrestien, 2001, p. 702.
[29] B. PLESSIX, *Droit administratif général*, 2e éd., LexisNexis, 2018, p. 774.
[30] CE, 23 janvier 1953, Naud, Rec. p. 32 ; CE, 29 juillet 1953, Damazière, Rec., p. 407.
[31] CE, 8 juillet 1992, Ville de Chevreuse, n° 80775, Rec. ; CE, 29 décembre 1997, Maugendre, n° 164299, Rec. T.826

constitue également une facilité rédactionnelle lui permettant de ne pas rappeler les diverses circonstances de l'espèce pourtant utiles à la compréhension de sa décision[32].

Dans l'arrêt de principe en la matière, le Conseil se limite à considérer « *qu'il résulte de l'instruction que l'éventualité de troubles, alléguée par le maire de Nevers, ne présentait pas un degré de gravité tel qu'il n'ait pu, sans interdire la conférence, maintenir l'ordre en édictant les mesures de police qu'il lui appartenait de prendre* »[33]. Le juge n'est ici guère éclairant sur les éléments dont disposait l'autorité de police l'ayant conduit à prédire une atteinte à l'ordre public à l'occasion d'une conférence littéraire consacrée à Courteline et Sacha Guitry. Les conclusions du commissaire du gouvernement enseignent que l'édile avait reçu le secrétaire local du syndicat national des instituteurs, qui lui avait remis une lettre l'informant d'une manifestation des instituteurs le jour de la conférence en cause afin que M. Benjamin, « *militant patronné par l'Action française* », ait connaissance de leurs sentiments à son égard, lettre relayée par des tracts, affiches et articles de presse. Le commissaire a toutefois estimé « *qu'il n'y avait pas à Nevers d'indices suffisants pouvant faire craindre des atteintes à l'ordre public de nature à justifier une décision d'interdiction* », et ce, en dépit de « *faits graves* » qui se seraient déroulés à l'occasion d'une précédente réunion publique à Saint-Etienne.

L'exemple historique du contrôle des mesures de police administrative éclaire sur la méthodologie mise en œuvre par le juge. Afin de s'assurer de la régularité de la prédiction de l'autorité administrative, le juge va lui-même peser la valeur probante des éléments dont elle disposait pour apprécier la nécessité d'édicter une mesure de police. En ce sens, le commissaire du gouvernement Lagrange exige, pour justifier l'interdiction d'une réunion publique, la réunion de « *circonstances objectives de nature à faire craindre des troubles graves* »[34]. L'administration ne peut se contenter d'hypothèses, de possibilités ou d'impressions ; elle doit se fonder sur des faits et des indications précises.

[32] Y. GAUDEMET, *Les méthodes du juge administratif*, thèse, LGDJ, BDP, t. 108, 1972, p. 106.
[33] CE, 19 mai 1933, Benjamin, Rec., p. 541, *S*. 1934 III, p. 1, concl. G. Michel, note A. Mestre ; P.-H. PRÉLOT, « L'actualité de l'arrêt Benjamin », *RFDA* 2013, p. 1020.
[34] M. LAGRANGE, concl. sur CE, 5 février 1937, Bujadoux, *D*. 1938 III, p. 20.

A cet égard, le contrôle du juge administratif en matière d'arrêtés interdisant le port du burkini sur les plages s'avère particulièrement éclairant. Pour juger illégale l'interdiction édictée par le maire de Villeneuve-Loubet, le juge du référé-liberté près le Conseil d'Etat statuant en cause d'appel a détaillé les éléments avancés par lui sur l'atteinte à l'ordre public qu'il entendait prévenir : « *Il ne résulte pas de l'instruction que des risques de trouble à l'ordre public aient résulté, sur les plages de la commune de Villeneuve-Loubet, de la tenue adoptée en vue de la baignade par certaines personnes. S'il a été fait état au cours de l'audience publique du port sur les plages de la commune de tenues de la nature de celles que l'article 4.3 de l'arrêté litigieux entend prohiber, aucun élément produit devant le juge des référés ne permet de retenir que de tels risques en auraient résulté. En l'absence de tels risques, l'émotion et les inquiétudes résultant des attentats terroristes, et notamment de celui commis à Nice le 14 juillet dernier, ne sauraient suffire à justifier légalement la mesure d'interdiction contestée* »[35]. Dans le même sens, à Cagnes-sur-Mer, l'intervention d'une unique altercation avec une personne portant une telle tenue n'est pas apparue suffisante pour justifier l'édiction d'une mesure d'interdiction[36].

En revanche, la solution inverse retenue par la Cour administrative d'appel de Marseille à propos de l'arrêté édicté par le maire de Sisco a été clairement justifiée par les éléments de sa prédiction d'atteinte à l'ordre public : « *Considérant qu'il ressort des pièces du dossier que le maire de Sisco a pris l'arrêté contesté pour prévenir les troubles à l'ordre public susceptibles de se produire suite à la violente altercation survenue le 13 août 2016 au lieu-dit Marine entre un groupe de familles d'origine maghrébine dont, selon plusieurs témoignages concordants, les femmes portaient sur la plage une tenue dénommée " hijab " ou " burka ", et une quarantaine d'habitants de la commune ; que cette rixe a nécessité l'intervention d'une centaine de CRS et de gendarmes qui ont dû établir un périmètre de sécurité autour des trois familles afin d'éviter leur lynchage par la population et a abouti à l'hospitalisation de cinq personnes, ainsi qu'à l'incendie de trois véhicules ; que ces affrontements*

[35] CE, 26 août 2016, Ligue des droits de l'homme, n° 402742, Rec. 15 janvier 2017
[36] CE, 26 septembre 2016, Ligue des droits de l'homme, n° 403578, Rec. T. 15 mai 2017

ont également donné lieu, le lendemain à Bastia, à une manifestation dans une atmosphère très tendue ayant également entraîné l'intervention des forces de l'ordre et l'usage de gaz lacrymogènes ; que ces faits, en raison de leur nature et de leur gravité, étaient susceptibles de faire apparaître des risques avérés de troubles à l'ordre public justifiant légalement l'interdiction édictée par l'arrêté en litige de porter des tenues vestimentaires manifestant de manière ostentatoire une appartenance religieuse »[37].

Compte tenu de la gravité de la mesure d'interdiction qu'elle édicte, et du fait que les mesures de police administrative doivent être « *justifiées par la nécessité de sauvegarder l'ordre public* »[38], l'autorité de police administrative doit faire état des éléments précis sur lesquels elle s'est fondée pour supposer qu'une atteinte à l'ordre public allait intervenir. Le juge exercera sur ces faits un contrôle normal[39].

On retrouve cette même logique en matière de contrôle de l'obligation d'exercer le pouvoir de police administrative lorsque le juge caractérise un manquement de l'autorité de police dans l'édiction d'une mesure de police indispensable pour faire cesser un péril grave résultant d'une situation particulièrement dangereuse pour l'ordre public[40]. Dans un tel cas, le juge reproche à l'administration ne pas avoir mis en œuvre son pouvoir de police alors que l'atteinte à l'ordre public résulte d'une prédiction certaine. Au regard des éléments à sa connaissance, une atteinte à l'ordre public était inévitable et la mesure préventive de police administrative devait impérativement être adoptée.

Sur un terrain indemnitaire, la responsabilité de la commune de Tanneron a été engagée pour défaut d'aménagement d'un dispositif permettant d'alerter rapidement un centre de secours à proximité d'un lieu de baignade particulièrement fréquenté, en dépit de plusieurs accidents antérieurs (quatre

[37] CAA Marseille, 3 juillet 2017, Ligue des droits de l'homme, n° 17MA01337.
[38] CC, 13 mars 2003, n° 2003-467 DC, § 9 ; CC, 10 mars 2011, n° 2011-625 DC, § 50 ; CC, 5 octobre 2012, n° 2012-279 QPC, § 15.
[39] J. PETIT, « Police administrative », *in Traité de droit administratif*, P. GONOD, F. MELLEREY, P. YOLKA (dir.), Dalloz, 2011, p. 41.
[40] CE, 23 octobre 1959, Doublet, Rec., p. 540, *RDP* 1959, p. 1235, concl. A. BERNARD, 1960, p. 802, note M. WALINE.

décès au cours des quatre années précédentes et quatre cas d'hydrocution dans les deux mois avant l'accident), rendant le décès d'un mineur de 16 ans par noyade inévitable[41]. Comme l'explique le commissaire du gouvernement Boyon, la vigilance du maire aurait dû être renforcée par la fréquence des accidents. Dans le même sens, la responsabilité de la commune de Bagnères-de-Bigorre a été engagée pour n'avoir pas mis en place de dispositif de signalisation et de protection d'un immeuble implanté à l'extrémité d'une piste verte de ski, et ce alors que deux accidents antérieurs étaient intervenus, rendant inévitable l'accident subi par une fillette de 8 ans[42]. De même, en raison d'un épisode de forte pluie annoncé par les services de météorologie, la Commune des Abymes aurait également dû interdire l'accès à un pont connu pour être inondable et dépourvu de garde-corps, ce qui aurait assurément permis d'empêcher que le véhicule de plusieurs usagers ne soit emporté par les eaux, entraînant leur décès[43].

En excès de pouvoir, le juge administratif peut contraindre les édiles locaux à mettre en œuvre leur pouvoir de police afin de conforter une falaise dont le risque d'effondrement a été établi par un rapport d'expertise, et de protéger les habitants des constructions implantées en contre-bas[44]. Il peut encore enjoindre au maire d'une commune d'ordonner l'enlèvement de matériaux combustibles et plastiques, de plusieurs véhicules à l'état d'épave, et de l'installation irrégulière de caravanes et de mobile homes, générateurs de nuisances eu égard au risque d'incendie et de pollution des sols qui en résulte ainsi qu'au trouble de la tranquillité du voisinage qu'ils engendrent[45]. Au regard des éléments du dossier, le juge considère comme certaine la prédiction de l'atteinte future à l'ordre public.

Le juge des référés peut également contraindre l'autorité de police lorsqu'il ressort des éléments qui lui sont soumis qu'une atteinte à la dignité de la personne humaine est déjà prégnante et ne fera que perdurer en raison de l'insuffisance des points d'eau, des latrines, des douches, et d'un dispositif de

[41] CE, 13 mai 1983, Lefebvre, n° 30538, Rec., *AJDA* 1983, p. 476, concl. M. Boyon.
[42] CAA Bordeaux, 11 octobre 2018, n° 16BX02647.
[43] CAA Bordeaux, 16 mai 2017, n° 15BX00859.
[44] CAA Bordeaux, 11 décembre 2017, n° 13BX02426.
[45] CAA Bordeaux, 16 janvier 2014, Commune d'Ambès, n° 13BX00105.

collecte des ordures dans la « jungle » de Calais[46]. Cette intervention du juge des référés permet désormais au justiciable, dans son principe, de ne plus subir de victoire à la Pyrrhus, telle que celle de l'arrêt Benjamin, dans laquelle le juge sanctionne l'illégalité d'une mesure d'interdiction trois ans après les faits[47]. Elle n'est néanmoins pas exempte de critiques en ce qu'elle restreint pour le justiciable les garanties du principe de la contradiction et des voies de recours[48].

Si certains ont pu plaider pour un approfondissement du contrôle des décisions de refus de mise en œuvre du pouvoir de police administrative[49], une telle évolution ne nous paraît pas souhaitable. Il revient en effet indéniablement au juge de sanctionner la méconnaissance par l'autorité administrative de ses pouvoirs de police lorsqu'une atteinte à l'ordre public est certaine, mais en aucun si elle s'avère seulement possible. En d'autres termes, le contrôle des éléments de la prédiction de l'atteinte à l'ordre public permet au juge de contrôler la nécessité de la mesure de police administrative mais non son opportunité, qui ne relève pas de l'office du juge administratif[50]. Comme Paul Bernard a pu l'exposer dans sa thèse il y a plus de cinquante ans, le contrôle du juge sur les circonstances de fait constitue la limite intérieure de l'action administrative en matière de police[51].

II) Le contrôle du contenu de la prédiction

La mesure de police doit être « *strictement nécessaire* »[52] au maintien de l'ordre public, en ce sens que « *la décision ne doit pas excéder ce qu'exige la réalisation du but poursuivi* » ; l'administration doit justifier que l'objectif ne pouvait pas être atteint par l'édiction d'une mesure moins attentatoire aux

[46] CE, 23 novembre 2015, Ministre de l'intérieur c/ Associations Médecins du monde et Secours Catholique, n° 394540, Rec. ; CE, 31 juillet 2017, Commune de Calais, n° 412125, Rec.
[47] A. CIAUDO, « L'office du juge administratif de l'urgence : libre propos sur un carcan juridictionnel *», in Le renouvellement de l'office du juge administratif*, J.-F. Lafaix (dir.), Berger-Levrault, 2017, p. 180.
[48] X. PRÉTOT, C. ZACHARIE, *La police administrative*, LGDJ, 2018, p. 140.
[49] F. MELLERAY, « L'obligation de prendre des mesures de police initiales », *AJDA* 2005, p. 71.
[50] P. DELVOLVÉ, « Existe-t-il un contrôle de l'opportunité ? », *in Conseil constitutionnel et Conseil d'Etat*, LGDJ-Montchrestien, 1988, p. 293.
[51] P. BERNARD, *La notion d'ordre public en droit administratif*, thèse, LGDJ, BDP, t. 42, 1962 p. 110.
[52] CE, 19 février 1909, Abbé Olivier, *Rec*., p. 180, concl. P. CHARDENET ; CE, 11 juin 2012, Commune de l'Etang salé, n° 360024, Rec. T.

libertés[53]. C'est en ce sens que l'ordre public peut être qualifié de « *norme de nécessité* »[54]. L'analyse de la jurisprudence en matière de contrôle des mesures d'interdiction des manifestations et spectacles laisse transparaître la récurrence du reproche émis à l'encontre de l'autorité de police de ne pas avoir fait primer la liberté face aux contraintes de l'ordre public. Le commissaire du gouvernement Corneille exposait de manière solennelle que « *le point de départ de notre droit public est dans l'ensemble des libertés des citoyens, que la Déclaration des droits de l'homme est explicitement ou implicitement au frontispice des Constitutions républicaines et que toute controverse de droit public doit, pour se calquer sur les principes généraux, partir de ce point de vue que la liberté est la règle et la restriction de police l'exception* »[55].

Il ne faut néanmoins pas perdre de vue la difficulté particulière du rôle de l'administration en la matière. Il est parfois facile de critiquer *a posteriori* l'absence d'interdiction par le constat des conséquences de la tenue d'une manifestation ayant débordé, tel un ancien Premier ministre indiquant depuis l'étranger que les violences et stigmates d'antisémitisme résultant de manifestations de « gilets jaunes » à l'hiver 2018-2019 auraient pu être évités par des mesures d'interdiction[56]. La décision apparaît sans doute moins aisée lorsque l'on se trouve placé dans l'étau entre d'une part la critique de l'atteinte aux libertés constitutionnelles de manifestation, de réunion et d'expression, et d'autre part la nécessaire protection de la sécurité publique.

Hauriou soulignait déjà au début du siècle dernier que le maintien de l'ordre public doit être assuré au moyen d'une « *sage réglementation* »[57]. Quelques années plus tard, Duez et Debeyre soutenaient que « *L'interdiction apparaît comme un ultima ratio à valider dans le seul cas où elle apparaît*

[53] J. PETIT, « Le contrôle juridictionnel des mesures de police par le juge administratif », *in La police administrative*, C. VAUTROT-SCHWARZ (dir.), PUF, 2014, p. 216 ; V. égal. H. de GAUDEMAR, « Le contrôle juridictionnel des mesures de police administrative », *in L'ordre public*, C.-A. Dubreuil (dir.), Cujas, 2013, p. 333.
[54] E. PICARD, *La notion de police administrative*, thèse, t. 2, LGDJ, BDP, t. 146, 1984, p. 544 et s. ; E. PICARD, « Police », *in Dictionnaire de la culture juridique*, D. ALLAND, S. RIALS (dir.), PUF, 2003, p. 1169.
[55] L. CORNEILLE, concl. sur CE, 10 août 1917, Baldy, Rec., p. 638.
[56] « Gilets jaunes : Valls aurait interdit les manifestations », *L'express*, 21 février 2019 ; V. égal. « Gilets jaunes : Eric CIOTTI appelle à interdire les manifestations », *Le Parisien*, 17 février 2019.
[57] M. HAURIOU, *Précis de droit administratif et de droit public*, 12e éd., Sirey, 1933, réimp., Dalloz, 2002, p. 549.

comme étant la seule ressource pour empêcher des troubles graves auxquels conduirait l'exercice de la liberté »[58].

S'il est certain que l'appréciation de la nécessité d'une mesure de police est inévitablement emprunte de subjectivité[59], la nécessité d'édicter une mesure d'interdiction résultera d'une appréciation concrète et casuistique des éléments d'information sur les troubles probables susceptibles d'intervenir à raison de la tenue effective d'une manifestation ou d'un spectacle et de l'impossibilité pour l'administration d'assurer la sécurité publique par d'autres moyens que l'interdiction. Comme le soulignait la commissaire du gouvernement Michel dans ses conclusions sur l'arrêt Benjamin, une manifestation ne peut être interdite s'il est seulement prévisible qu'elle sera « orageuse », ou seulement « effervescente » pour reprendre l'expression d'Achille Mestre dans sa note sous le même arrêt.

C'est en ce sens et au regard des éléments dont disposait l'administration que le Conseil d'Etat a estimé illégales en raison de l'absence de débordements prévisibles : l'interdiction d'une réunion présidée par Charles Maurras, en dépit de la dissolution antérieure des ligues de l'Action Française[60] ; l'interdiction de réunions du parti communiste contre la guerre d'Indochine[61] ; l'interdiction de l'Université d'été du Front national à Annecy[62]. En revanche, eu égard aux risques de débordements et d'envahissement d'un hôpital déjà provoqués par l'association organisatrice, ainsi que des menaces et intimidations sur des médecins et des patientes, l'interdiction d'une manifestation anti-avortement a été considérée comme légale[63]. Il en a été de même pour l'interdiction de la manifestation de l'association « Collectif 69 de soutien au peuple palestinien » à l'occasion d'un match de basket-ball d'une équipe israélienne, l'administration s'étant expressément fondée sur une note blanche des services de renseignement faisant état de risques d'affrontements sérieux et

[58] P. DUEZ, G. DEBEYRE, *Traité de droit administratif*, Dalloz, 1952, p. 519.
[59] R. CHAPUS, *Droit administratif général tome 1*, 15e éd., Montchrestien, 2001, p. 731.
[60] CE, 5 février 1937, Bujadoux, Rec., p. 153, *D*. 1938, III, p. 19, concl. M. LAGRANGE.
[61] CE, 29 juillet 1953, Damazière, Rec., p. 407.
[62] CE, 19 août 2002, Front national, n° 249666, Rec. 311.
[63] CE, 30 décembre 2003, Lehembre et Association SOS tout-petits, n° 248264, Rec. T. 888 ; CAA Paris, 23 mars 2000, Association SOS tout-petits, n° 98PA04534.

de la mobilisation des forces de l'ordre sur d'autres tâches à raison de l'intervention récentes des attentats de Paris[64].

Le contrôle juridictionnel du contenu de la prédiction de l'atteinte à l'ordre public s'avère encore plus ardu en matière de protection de l'ordre public immatériel[65]. Lorsque la personnalité clivante d'un conférencier ou la teneur de ses propos sont contestés au regard de l'atteinte potentielle à la dignité de la personne humaine ou des valeurs fondamentales de la République, l'autorité de police peut intervenir pour préserver une atteinte à l'ordre public. On retient récemment en ce sens la tentative avortée d'interdire une conférence de Tariq Ramadan devant le juge des référés du Tribunal administratif de Nice, au motif que l'intéressé « *n'a jamais fait l'objet de poursuites pénales* » ni tenu « *des propos de nature à porter des atteintes graves au respect des valeurs et principes consacrés par la Déclaration des droits de l'homme et du citoyen et par la tradition républicaine* »[66]. Compte tenu des propos tenus par l'islamologue à propos de la lapidation des femmes, l'anormalité des homosexuels, et la justification des discriminations entre hommes et femmes, cette assertion s'avère pour le moins contestable.

On peine à comprendre la cohérence d'une telle décision à l'aune de l'admission par le Conseil d'Etat de la censure des spectacles de Dieudonné[67]. Alors que l'humoriste avait souligné qu'il expurgerait son spectacle « Le mur » des « propos pénalement répréhensibles et de nature à mettre en cause la cohésion nationale » afin d'éviter toute atteinte à la dignité de la personne humaine, le Conseil d'Etat a validé la stratégie du Ministre de l'intérieur, M. Valls, d'une « censure préalable »[68]. La prédiction s'avère pour le moins sujette à caution lorsque la mesure de police administrative vise à interdire des propos qui ne seront pas tenus. Si le Conseil d'Etat assume la composante uniquement immatérielle du trouble qui résulterait des propos de l'humoriste[69], il omet de

[64] CAA Lyon, 24 octobre 2017, Association « Collectif 69 de soutien au peuple palestinien », n° 16LY02638.
[65] P. DELVOLVÉ, « L'ordre public immatériel », *RFDA* 2015, p. 890 ; M.-O. PEYROUX-SISSOKO, *L'ordre public immatériel en droit public français*, thèse, LGDJ, BCSP, t. 149, 2018, p. 470 et s.
[66] « Si vous n'avez rien suivi à la polémique autour de la venue de Tariq Ramadan sur la Côte d'Azur », *Nice-Matin*, 18 mars 2016.
[67] CE, 9 janvier 2014, Ministre de l'intérieur c/ Dieudonné, n° 374508, Rec. 1
[68] B. SEILLER, « La censure a toujours tort », *AJDA* 2014, p. 129.
[69] M. GUYOMAR, « Nouveaux enjeux de l'ordre public et pouvoir de police », *in L'ordre public*, La documentation française, 2018, p. 62.

rappeler que les propos qu'il entend proscrire n'auraient pas été proférés. La nécessité de la mesure de police perd ici son fondement même en raison de l'impossible réalisation de la prédiction de l'atteinte à l'ordre public. Au lieu de reposer sur une prédiction résultant de la réunion d'indices concordants, la mesure de police constitue une censure préventive comprenant un fort risque de dérapage et d'arbitraire[70] puisqu'elle est fondée sur la supposition de la commission future d'une infraction.

Comme s'en inquiète justement et légitimement le professeur Gohin, la restriction de la liberté de réunion au nom de la protection de la dignité de la personne humaine suppose de mieux définir cette notion à contenu si variable afin de ne pas risquer une « *hiérarchie insupportable ou le tri inacceptable parmi les victimes de l'inhumain, entre ceux qu'il faut justement plaindre et ceux qu'il faudrait injustement taire, c'est venir distinguer entre les génocides ou les traites ou les esclavages ou encore les discriminations à l'encontre des minorités les plus diverses* »[71]. A l'instar de certaines associations qui défendent une conception de la laïcité à géométrie variable[72], le juge administratif pourrait être tenté, par la mise en œuvre de ce contrôle du spectacle attentatoire à la dignité de la personne humaine, de retenir une conception subjective et discriminante de cette dignité. L'analyse comparée des deux décisions précitées invite à s'interroger sur la nécessité d'interdire *a priori* des potentiels propos antisémites et négationnistes mais d'autoriser des propos homophobes, misogynes et justifiant des actes de torture inhumains et dégradants. En s'arrogeant la possibilité de contrôler l'atteinte à la dignité de la personne humaine, le Conseil d'Etat a ouvert la boîte de Pandore, l'inclusion de cette notion dans l'ordre public général comportant « le double danger de l'incertitude et de l'absolu »[73].

*

* *

[70] E. SIRE-MARIN, « Dieudonné : l'arrêt « Minority report » du Conseil d'Etat », *Slate.fr*, 10 janvier 2014.
[71] O. GOHIN, « Liberté d'expression, liberté de réunion, police administrative et ordre public : l'affaire *Dieudonné* », *RFDA* 2014, p. 87.
[72] A. CIAUDO, « Les crèches de Noël dans les bâtiments publics : la messe est dite », *Le journal du droit administratif*, Dossier 3, 2017, *Les Cahiers de la Lutte contre les discriminations*, n° 3, L'Harmattan, 2017, p. 59.
[73] J. PETIT, « Les ordonnances *Dieudonné* : séparer le bon grain de l'ivraie », *AJDA* 2014, p. 866.

Dans son contrôle de la nécessité des mesures de police administrative, le juge administratif exige de l'autorité administrative qu'elle justifie des éléments en sa possession lui faisant présager d'une atteinte future à l'ordre public. Il doit à ce titre exercer un contrôle strict sur la certitude de la concrétisation de la prédiction administrative. Ce contrôle doit être le même qu'il s'agisse de protéger l'ordre public matériel comme immatériel, sans succomber à la tentation de la censure préventive au regard de la seule commission passée d'infractions pénales. A défaut, il devra justifier des discriminations qu'il instaure lui-même entre les différentes catégories d'atteintes à la dignité de la personne humaine. Pour reprendre une formule du doyen Hauriou, toujours emprunte de sagesse : « *Nous avons en France la manie de la formule générale. Elle est quelquefois une garantie de l'égalité, mais trop souvent, elle est un péril pour nos libertés qui se trouvent restreintes plus qu'il n'était nécessaire, elle recouvre une certaine paresse d'esprit qui dispense d'analyser exactement les situations* »[74].

[74] M. HAURIOU, note sous CE, 7 mai 1926, Sourisse, *S*. 1926 III, p. 41, *Notes d'arrêts*, La mémoire du droit, 2000, t. 2, p. 546.

Pouvons-nous consentir à un avenir meilleur lorsque nous sommes rattrapés par le « pire » du passé ?

Karine FAVRO

Maître de conférences en droit public HDR,
Université de Haute-Alsace
CERDACC (EA 3992)

Le consentement. Concept fondamental du droit, le consentement procède d'une manifestation de volonté consistant à engager juridiquement une personne, des biens ou les deux à la fois, essentiellement pour l'avenir[75]. En cela, le consentement permet la projection d'une situation au regard d'éléments ou d'évènements passés. La manifestation de volonté doit être exempte de vices, non équivoque, et prend selon les cas, la forme d'une acceptation, poignée de mains ou autre manifestation affective, d'une autorisation, d'un agrément, d'une ratification, d'un silence ou autre manifestation juridique. Il existe donc différentes manières de consentir mais bien souvent les effets de ce consentement sont illusoires. L'illusion tient au fait que la personne consentante n'a pas tous les éléments pour consentir, soit parce qu'ils existent, et qu'ils ne lui ont pas été délivrés ou imparfaitement délivrés, soit parce qu'ils n'existent pas encore ou que ce consentement n'a pas lieu d'être…

C'est la raison pour laquelle le consentement est généralement affublé d'un qualificatif, sorte de syntagme figé, car ce consentement doit être éclairé, libre, spécifique, indubitable, explicite, informé, etc[76]. Exprimant ainsi que celui qui consent, dispose des éléments pour consentir valablement, tout en saisissant les limites et les effets. Le consentement doit être valable pour produire des

[75] Le consentement peut en effet, avoir un effet rétroactif notamment dans le domaine du droit des sociétés ou dans le cadre du contrat de mandat.
[76] Avis du G29 n° 15/2011 (WP187) du 13 juillet 2011 sur la définition du consentement ; Lignes directrices sur le consentement, élaborées par le G29, au sens du règlement 2016/679 du 10 avril 2018.

effets juridiques. C'est dans le domaine de la formation du contrat ou en droit médical que le consentement a fait l'objet des développements les plus conséquents[77]. Apparemment, certaines conditions de forme constitueraient la preuve irréfutable de l'engagement contractuel, tel qu'un échange physique des consentements lors d'un mariage, par exemple. En matière médicale, le patient devrait être en mesure de comprendre le diagnostic et de manifester son consentement libre et éclairé sur sa volonté de savoir ou de ne rien savoir de son état de santé[78]. Ce consentement supposerait au préalable que soient délivrées des informations loyales, claires et adaptées à son degré de compréhension de la part des équipes soignantes et médicales, libre de toute pression ou contrainte. L'équipe médicale ne serait déliée de l'obligation d'information seulement si le patient est en mesure de manifester sa volonté[79]. Seule l'urgence et l'impossibilité de requérir le consentement des représentants légaux constitueraient des dérogations au principe du consentement[80], etc.

Rappelé ainsi en quelques phrases, le consentement relèverait de l'évidence pour la société du XXIème siècle consumériste, individualiste, en capacité de décider ou à tout le moins en ayant le sentiment d'y parvenir. Aussi, la réflexion en droit sur le consentement peut-elle paraître éculée[81]. Cependant, le seul fait de renforcer la prise en compte du consentement par des qualificatifs, justifie l'emploi du conditionnel dans la description des situations susmentionnées, car

[77] J. GHESTIN, G. LOISEAU, Y.-M. SERINET, *La formation du contrat : le contrat, le consentement*, 4e édition - Tome 1, LGDJ, 2013 ; R. SIRI, *La théorie générale des vices du consentement, entre mythe et réalité ?*, PUAM, Centre Pierre Kayser, mai 2008 ; E. RASCHEL, *La pénalisation des atteintes au consentement dans le champ contractuel*, Thèse, PUJP, novembre 2014 ; G. FRANCOIS, *Consentement et objectivation – L'apport des principes en droit européen du contrat à l'étude du consentement contractuel*, Institut de droit des affaires, PUAM, avril 2007 ; J.-P. DEPOIX, sous la dir. de, *Droits et place des personnes soignées à l'hôpital*, Lamarre, mars 2019 ; Association Française de Droit de la Santé, *Consentement et santé*, Dalloz, Thèmes & commentaires, avril 2014 ; G. NICOLAS, A.-C. RÉGLIER, *Mort et droit de la santé : les limites de la volonté*, LEH Éditions, décembre 2016 ; M. BENILLOUCHE, X. CABANNES, sous la dir. de, *Hospitalisations sans consentement*, CEPRISCA, PUF, mars 2013 ; S. THÉRON, *Les soins psychiatriques sans consentement – législation, droits et libertés du patient, modalités de prise en charge du patient, responsabilité des intervenants*, Dunod, octobre 2017 ; D. DARMSTÄDTER-DELMAS, *Les soins psychiatriques sans consentement – Dispositif juridique, procédure, jurisprudence, conseils pratiques*, LexisNexis, avril 2017 ; N. GILOUX, M. PRIMEVERT, sous la dir. de, LEH Editions, février 2017 ; B. EYRAUD, L. VELPRY, P. VIDAL-NAQUET, *Contrainte et consentement en santé mentale – Force, influencer, coopérer*, PUR, octobre 2018.

[78] CE, ord, 8 septembre 2005, n°284803 ; CE, 26 juillet 2017, n° 412618.

[79] CSP, art. L.1111-2, R.4127-35 de ce code repris par l'article 35 du code de déontologie médicale.

[80] CSP, art. L. 1111-4.

[81] La doctrine s'évertue à démontrer l'inverse : *Le consentement*, Actes de colloque de l'École doctorale Droit et Science politique, CREAM, juin 2018 ; S. BESSON, Y. MAUSEN, P. PICHONNAZ, *Le consentement en droit*, Schulthess, janvier 2019 ;

cela constitue la preuve que le consentement ne se suffit pas à lui-même pour emporter la conviction. Le réalisme en la matière montre que le droit ne peut se saisir intégralement de cette question ; garantir juridiquement l'expression du consentement ne suffit pas, il faut le conscientiser. Les apparences peuvent masquer la contrainte ou l'imprévisibilité d'une situation[82]. Il existe parfois un décalage important entre le comportement physique et psychologique pouvant d'emblée vicier le consentement[83]. Cependant, ériger le consentement en principe juridique dans ce contexte, procède de la volonté d'informer la personne concernée qu'il s'agit d'un acte marquant la protection de ses droits les plus fondamentaux, l'alertant sur la nécessité d'y prêter attention. Dès lors, l'affirmation de ce principe doit s'accompagner du développement complémentaire de comportements éthiques pour réduire ou neutraliser les effets de la contrainte ou plus simplement les biais, comme la gestion de la douleur ou l'éthique des soins en matière médicale. Dans d'autres cas, il s'agira, en complément, de développer l'information préalable de la personne concernée et de la conscientiser sur l'environnement auquel le consentement est attaché afin de lui permettre d'acquérir cette capacité d'agir.

L'apport du RGPD. Ce constat procède désormais de l'octroi du consentement associé à des traitements de données personnelles, effectués instantanément et reposant de plus en plus souvent sur des algorithmes auto-apprenants. A chaque connexion, la traçabilité de l'individu est avérée et permet progressivement d'enfermer l'utilisateur de demain dans un profil préétabli en le contraignant ou en l'incitant à l'aide de *nudges*[84] à ne pas s'en écarter. La bulle algorithmique désigne la finalité du processus, c'est-à-dire « *l'état d'isolement intellectuel et culturel dans lequel un internaute se retrouve lorsque les informations qu'il reçoit sur Internet sont uniquement ciblées en*

[82] « *Que faire d'une liberté dont on ne se prévaut pas tant que cela, dans un contexte où maladie et médecine s'imposent de fait au patient ? Et quelle compréhension, quelle clarté investir quand, d'emblée, tout est bousculé et confus ? Les valeurs du jugement réfléchi ne semblent pas vraiment stimulées quand on ne sait plus ni où on en est ni ce qui peut advenir dans la maladie. De même, la vulnérabilité physique et psychique qui caractérise la situation de patient ne laisse guère place à une pleine jouissance de la liberté, pas plus qu'elle n'autorise un éclairage complet de la scène et des enjeux du drame* » ; N. PÉLICIER, « Un consentement pleinement libre et éclairé ? », LAENNEC, 2011/4, t.59, p.24.

[83] V. NDIOR (sous la dir. de), *Les mariages forcés et le droit*, Institut universitaire de Varenne, Colloques & Essais, juillet 2018.

[84] CNIL, *La forme des choix : données personnelles, design et frictions désirables*, 6e Cahier IP, 2019, p.19.

fonction de son profil »[85]. Il s'agit de collecter des données et métadonnées dans le but de surveiller, contraindre, inciter, leurrer, interdire aux individus certains comportements et d'adapter les informations reçues aux comportements des internautes, à leurs opinions ou leurs choix politiques, conséquences du modèle économique de l'Internet et de ses services gratuits.

Consentement et fondements légitimes. Le rôle du consentement a été expressément reconnu à l'article 8, paragraphe 2 de la Charte des droits fondamentaux de l'Union européenne, prévoyant que les données à caractère personnel peuvent faire l'objet d'un traitement « loyal » à des fins déterminées, sur le fondement du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Au titre de ces fondements qui résultent du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 dit RGPD, se trouvent la sauvegarde de la vie humaine, l'exécution d'un contrat, le respect d'une obligation légale, l'exécution d'une mission de service public ou la réalisation par le responsable du traitement d'un intérêt légitime dont on mesure l'étendue[86].

Certes, aux termes de l'article 6 de ce texte, le consentement n'est pas une obligation préalable à toute collecte de données personnelles, et les autres fondements légitimes permettent aux responsables de traitement d'y échapper notamment parce qu'il s'agit d'exécuter un contrat ou d'assurer des intérêts légitimes. Cela dit, si le responsable souhaite échapper au consentement, il est tenu d'informer la personne du fondement juridique sur lequel repose le traitement. L'application de l'une de ces bases juridiques doit être établie avant l'activité de traitement et en lien avec une finalité spécifique. A l'inverse, s'il choisit le consentement, il doit en évaluer tous les effets, y compris le retrait[87]. En outre, il est théoriquement impossible de passer d'une base juridique à une autre lorsque la validité du consentement est en cause, simplement pour

[85] C. CASTELLUCCIA, « La « datapulation » ou la manipulation par les données », *La Revue européenne des médias et du numérique*, hiver 2018-2019, n°49, p.92.

[86] J. FRAYSSINET, « Le projet de loi relatif à la protection des personnes physiques à l'égard des traitements des données à caractère personnel : constances et nouveautés », *CCE*, janvier 2002, p.12 ; A. LEPAGE, « Consentement et protection des données à caractère personnel », in J.-L. GIROT, sous la dir. de, *Le harcèlement numérique*, Dalloz, 2005, p.231 ; N. METALLINOS, « Les apports du règlement général relatif à la protection des données personnelles sur les conditions de licéité des traitements », *Dalloz IP/IT* 2016, p.588.

[87] Bien que la personne concernée puisse retirer son consentement à tout moment sans compromettre pour autant la licéité du traitement fondé sur ce consentement.

justifier auprès de la personne concernée, du traitement de ses données[88]. Le consentement constitue dans l'esprit du texte, la meilleure protection de la personne qui aurait donc le « choix » de consentir ou non à la collecte et à l'usage de ses données essentiellement, d'ailleurs, à l'égard des services gratuits massivement utilisés. Pour s'en assurer, ce consentement doit précisément être périodiquement renouvelé laissant ainsi à la personne concernée, une seconde chance d'y procéder avec détermination… mais sans remettre en cause le passé.

Reste que le responsable de traitement ne doit pas fonder le traitement des données sur le consentement, si le traitement repose en tant que tel, sur d'autres bases juridiques ce qui serait « *fondamentalement déloyal envers les personnes concernées* »[89]. Plus encore, le consentement pourrait dissimuler la volonté du responsable du traitement d'élargir son champ à des traitements plus hasardeux, risqués qui ne pourraient se prévaloir d'aucun fondement légitime…

Algorithmes et pouvoir de décision. A ce titre, l'article 22 du RGPD précise que « *la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* », sauf si, précise le texte, ce traitement est « *fondé sur le consentement explicite de la personne concernée* ». Le consentement peut donc justifier le profilage et plus largement la prise de décision fondée sur traitement algorithmique, même lorsqu'il produit des effets juridiques. Le droit français va d'ailleurs au-delà des marges de manœuvre consenties aux États membres, en autorisant notamment l'administration a prendre des décisions individuelles sur le seul fondement d'un traitement automatisé, dans le respect de l'article L.311-3-1 du CRPA[90]

[88] Lignes directrices sur le consentement, élaborées par le G29, au sens du règlement 2016/679 du 10 avril 2018.

[89] *Ibidem*.

[90] Article 47, LIL révisée : « Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne.

« Aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris le profilage, à l'exception :

« 1° Des cas mentionnés aux a et c du 2 de l'article 22 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, sous les réserves mentionnées au 3 du même article 22 et à condition que

sous réserve que le responsable de traitement « *s'assure de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard* ». Un tel dispositif semble exclure les algorithmes auto-apprenants[91], mais ne précise pas à quel moment la personne est informée et de quelle manière se manifeste la maîtrise du processus. Le dispositif national s'écarte, par ailleurs, du droit consacré par le RGPD, pour y substituer une interdiction dont les contours ne sont pas totalement définis[92].

Envisagé sous cet angle, le consentement constitue une sorte de blanc-seing pour accéder au service, que l'on pourrait assimiler à un vice du consentement en ce qu'il instaure un rapport de force, en principe proscrit par le RGPD. Ce rapport de force est d'autant plus virulent qu'il met en tension les principes de protection des données personnelles et les enjeux du *big data*[93]. La réponse « textuelle » viserait à systématiser le consentement pour l'ensemble des traitements fondés directement sur des algorithmes de façon à informer les personnes concernées. A ce titre, le projet de règlement « vie privée et communications électroniques »[94] en lien avec l'appréciation du consentement aux termes du RGDP, a pour objet d'instaurer le consentement, comme le précise le groupe des régulateurs européens, au sein des lignes directrices, « *pour la plupart de leurs messages commerciaux en ligne et de leurs appels*

---

les règles définissant le traitement ainsi que les principales caractéristiques de sa mise en œuvre soient communiquées, à l'exception des secrets protégés par la loi, par le responsable de traitement à l'intéressé s'il en fait la demande ;

« 2° Des décisions administratives individuelles prises dans le respect de l'article L. 311-3-1 et du chapitre Ier du titre Ier du livre IV du code des relations entre le public et l'administration, à condition que le traitement ne porte pas sur des données mentionnées au I de l'article 6 de la présente loi. Ces décisions comportent, à peine de nullité, la mention explicite prévue à l'article L. 311-3-1 du code des relations entre le public et l'administration. Pour ces décisions, le responsable de traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard.

« Par dérogation au 2° du présent article, aucune décision par laquelle l'administration se prononce sur un recours administratif mentionné au titre Ier du livre IV du code des relations entre le public et l'administration ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel. »

[91] Cons. Const. n° 2018-765 DC, 12 juin 2018.

[92] V. le commentaire du dispositif, J. ROCHFELD, « Le consentement des décisions prises par algorithme », *Dalloz IP/IT 2018*, p.474.

[93] J. SCHWEIGER, « Smart cities et nouveaux enjeux de protection des données : comment tirer profit du nouveau règlement européen ? », *Dalloz IP/IT* 2017 p.624.

[94] Proposition de Règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), COM/2017/010 final - 2017/03 (COD).

commerciaux, ainsi que pour leurs méthodes de suivi en ligne, y compris moyennant l'utilisation de cookies, d'applications ou d'autres logiciels »[95]. Mais l'adoption de ce règlement est en souffrance faute de consensus.

Le consentement doit néanmoins porter le processus de protection des données dans la mesure où il doit reposer sur le respect des principes relatifs au traitement énoncés à l'article 5 du RGPD concernant la loyauté, la nécessité, la proportionnalité ainsi que la qualité des données. Il se justifie au regard d'une collecte, fonction de la finalité poursuivie et spécifique au traitement. En l'absence de quoi, le consentement présente un caractère abusif[96]. Le paradigme sur lequel repose le RGPD (le principe d'*accountability* - reddition de comptes des responsables de traitement - ou de *privacy by design* et *default* - protection de la vie privée dès la conception du contenu mis à disposition de l'internaute-) doit également guider l'obtention du consentement. Cette approche de gestion préventive du risque se retrouve dans l'obligation de protection des données et impose le recours aux technologies pour respecter des données personnelles dès la conception et tout au long de leur vie, jusqu'à leur élimination définitive. Ce processus permet de mettre en œuvre une politique de responsabilité quant à l'utilisation des données qui repose sur une démarche de *compliance*, et d'atteindre un équilibre entre protection et innovation. Elle s'inscrit dans une logique d'analyse de risque et d'adoption de barrières pour prévenir tout risque et garantir aux personnes concernées, un niveau de protection élevé.

L'apport de la CNIL en la matière : la Délibération *Google* de janvier 2019[97]. La question du consentement a cristallisé les débats lors de l'adoption du RGDP en raison de la détermination par les États du niveau d'information requis des personnes concernées. A ce titre, il y aurait encore à redire car cette information n'est, d'une certaine manière, jamais celle que l'on attend en ce qu'elle est plaquée à l'obtention du consentement alors qu'on la souhaiterait *a priori*, utile, facile d'accès, et davantage éducative. L'asymétrie informationnelle est caractérisée. C'est d'ailleurs ce que relève la CNIL dans sa

[95] Voir l'avis 03/2016 sur l'évaluation et la révision de la directive «vie privée et communications électroniques» (WP 240).

[96] Lignes directrices sur le consentement, élaborées par le G29, au sens du règlement 2016/679 du 10 avril 2018.

[97] Délibération de la formation restreinte n°SAN-2019-001 du 21 janvier 2019 prononçant la sanction pécuniaire à l'encontre de la société Google LLC : voir annexe.

délibération, extrêmement détaillée et à forte teneur pédagogique, visant *Google*, connue du grand public en raison du montant de la sanction prononcée : 50 millions d'euros. La CNIL retient que le consentement des utilisateurs de *Google* n'est pas suffisamment éclairé car l'information est diluée dans plusieurs documents. L'utilisateur ne peut prendre conscience de l'ampleur des traitements mis en œuvre, sauf à générer cinq à six actions de sa part, et à condition qu'il fasse preuve d'une navigation avertie. L'information requise n'est pas à la hauteur des traitements massifs mis en œuvre par *Google* de manière durable et continu au mépris de l'utilisateur. La gravité des manquements au RGPD est soulignée par la CNIL. Des lignes directrices[98] élaborées par le groupe composé des régulateurs européens, dit G29[99], accompagnent utilement la mise en œuvre du RGPD. Ces lignes directrices traitent, dans le cadre d'une approche qui se veut pédagogique, des conditions qui président à l'obtention du consentement, du niveau d'information requis et de la transparence attendue de la part du responsable de traitement. En filigrane apparaît toute la difficulté de dépasser une approche strictement juridique et déterministe pour prendre en considération, toutes les possibilités de contourner le texte du fait du traitement massif de données, morcelé au sein d'un certain nombre de services, sites et applications. Autrement dit, et dans notre cas de figure, ce n'est pas *Google* qui opère les traitements mais *Google search, YouTube, Google home, Google maps, Playstore, Google photo*, etc. Le paramétrage en devient impossible.

Une approche par le design des interfaces pourrait être mise en perspective pour gérer cette difficulté, car ce sont ces interfaces qui incitent les utilisateurs à l'action et la prise de décision. Pour la CNIL, l'interface est « *le premier objet de médiation entre la loi, les droits et les individus* »[100], invitant les acteurs, utilisateurs compris, à co-construire une éthique du design afin de protéger la vie privée par la donnée. Elle pourrait s'accompagner d'une approche par les neurosciences, envisagée par Adrien Bouvel dans le cadre de ce numéro, afin de découper plus finement les étapes cérébrales du consentement et de produire une éthique du paramétrage, ou à tout le moins des modèles compatibles avec le fonctionnement des individus et une information adaptée

[98] Avis du G29 n° 15/2011 (WP187) du 13 juillet 2011 sur la définition du consentement ; Lignes directrices sur le consentement, élaborées par le G29, au sens du règlement 2016/679 du 10 avril 2018.
[99] Remplacé depuis l'entrée en vigueur du RGPD, par le Comité européen de la protection des données.
[100] CNIL, *La forme des choix : données personnelles, design et frictions désirables*, 6e Cahier IP, 2019, p.30.

et *a priori.* Certes, il faudrait que cette approche serve cette fois-ci les intérêts des utilisateurs et non des responsables de traitement.

La manifestation du consentement par le droit d'opposition. Du fait de la collecte permanente de données sans liens apparents, le traitement précède souvent le consentement dans la mesure où l'une des fonctions du traitement consiste à anticiper, voire inciter ou contraindre les besoins de l'utilisateur[101], parfois positivement – lorsqu'il s'agit de détecter par exemple qu'une personne âgée est en situation de détresse et de sauver des vies[102]– parfois négativement – par l'identification de comportements à risque discriminant des individus ou des catégories d'individus.

Juridiquement pourtant, le moment du consentement est clairement identifié ; il doit être délivré avant le début du traitement des données ce qui le distingue du droit d'opposition qui intervient *a posteriori*. C'est ce droit d'opposition qui exerce finalement la fonction du consentement en validant « le non consentement » par la suppression du traitement. L'opposition peut être absolue dans le cadre d'un démarchage commercial, et pour motif légitime dans les autres cas[103]. L'opposition donne tout son sens au consentement. Le consentement doit être un acte positif, *a fortiori* pour le traitement des données les plus sensibles pour lequel il sera délivré sous forme écrite[104], mais cet acte dépendra de la transparence et du niveau d'information. Ce décalage entre le droit et la réalité n'est pas facile à prouver. Il est la résultante d'un processus contradictoire marqué par un traitement et un référencement constant des données collectées, parfois à partir de fondements supposés légitimes, mais qui en contrepartie appauvrissent progressivement les informations mises à disposition de l'utilisateur en fonction de ses traces de

[101] L. ARCELIN, « Données personnelles : sésame déterminant sur le marché de la publicité digitale », *Lamy Droit de l'Immatériel*, 1er novembre 2017, n°142.

[102] Le RGPD prévoit à ce titre, en son article 9, que le traitement des données de santé est interdit, sauf s'il est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, ou bien lorsque cette personne est dans l'incapacité physique ou juridique de délivrer son consentement.

[103] C. GALICHET, « Données professionnelles versus données personnelles – observations sous TGI Paris, 6 avril 2018, n°17/60436 », *Dalloz IP/IT 2018*, p.434 ; Cass. Civ. 1ère ch., 14 février 2018, n°17-10.499.

[104] L'article 114 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés précise que « *lorsque la recherche, l'étude ou l'évaluation nécessite l'examen des caractéristiques génétiques, le consentement de la personne concernée ou de ses représentants légaux doit être recueilli, préalablement au traitement, sous forme écrite. En cas d'impossibilité de le recueillir sous cette forme, le consentement exprès de la personne concernée est attesté par un tiers indépendant de l'organisme qui met en œuvre le traitement.* »

connexion, des incitations fournies par les *nudges* et l'urgence avec laquelle la personne concernée doit consentir pour obtenir le service ou le bien convoité. Mieux encore, l'utilisation du service ou l'obtention du bien pour lequel il a manifesté son consentement n'a pas été librement et préalablement choisi. Le risque reviendrait à considérer que la personne concernée est dotée d'une maîtrise à « l'autodétermination informationnelle », ce qui pourrait la rendre responsable de ses traitements et est contraire à la protection du droit des données personnelles[105]. En l'état, mais de tout temps, le consentement « *est contraint dans son périmètre et dans les obligations légales qui lui sont associées* », et induit une forme d'accommodement raisonnable pour concilier les intérêts de chacun[106] .

Consentement et démarche de compliance. Le consentement doit prendre la forme d'un instrument de contrôle mis au service de l'utilisateur, et ne doit pas avoir d'autres prétentions. L'environnement numérique qui fait de l'utilisateur un acteur à part entière, repositionne fermement la protection des données à caractère personnel sous l'angle du respect des droits de la personnalité avec toutes les conséquences que cela comporte[107]. Le pouvoir de police octroyé à la CNIL, en la matière, par la mise en œuvre du régime déclaratoire a été utilisé pendant des années pour protéger les utilisateurs contre eux-mêmes, et des traitements contraires aux principes posés par l'emblématique loi française Informatique et liberté du 6 janvier 1978 modifiée, atténuant ainsi les effets du consentement. Cependant, ce régime ne faisait plus sens. Mis en œuvre pour contrôler les conditions nécessaires à l'accès au marché et au respect des libertés[108], il n'est efficace que lorsque les moyens alloués sont fonction du nombre d'acteurs concernés et le contrôle, à un instant donné, suffisant. Or, c'est loin d'être le cas, les autorités administratives indépendantes (AAI) restant des administrations « légères », même en termes d'effectifs - 200 personnes[109]. Déresponsabilisant, ce régime de police a créé son lot de réfractaires, rétifs à la menace théorique du «

[105] N. OCHOA, « Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », *RFDA*, 2015, p.1157.
[106] CNIL, *La forme des choix : données personnelles, design et frictions désirables*, 6e Cahier IP, 2019, p.30.
[107] N. OCHOA, « Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », *RFDA*, 2015, p.1157.
[108] K. FAVRO, *op. cit.*
[109] A. DEBET, « Les nouveaux instruments de conformité », *Dalloz IP/IT* 2016, p.592 ; E. GABRIÉ, « Les pouvoirs des autorités de protection des données », *Dalloz IP/IT* 2017, p.268.

gendarme », et peu enclins à la nomination du correspondant informatique et libertés (CIL) pourtant nécessaire à l'application des principes posés par la loi informatique et libertés. En conséquence, la pédagogie visant à intégrer l'ensemble des acteurs, ce jusqu'au dernier maillon de la chaîne, à la démarche de mise en conformité, ne s'est jamais réellement opérée[110]. La nouvelle démarche devrait avoir pour effet, à terme, de compenser les défaillances structurelles de la CNIL en responsabilisant les acteurs au quotidien (à savoir les plateformes, les utilisateurs professionnels, les utilisateurs non profanes, mais également la CNIL)[111].

Sous l'effet du RGPD, cette loi a dernièrement été refondue du fait de l'intervention de la loi n°2018-493 du 20 juin 2018 et de l'ordonnance n°2018-1125 du 12 décembre 2018 qui est entrée en vigueur le 1er juin 2019[112]. Le pouvoir de police de la CNIL est supplanté par le jeu des acteurs, au titre desquels cette autorité de régulation est partie prenante, et par la mise en pouvoir d'agir des utilisateurs, autrement dit, l'empowerment. Dès lors, l'utilisateur dispose de ses données et fait valoir sa liberté de choix par l'apparente maîtrise d'un élément de sa personnalité ce qui se traduit par un droit subjectif dans ses composantes patrimoniales et extra-patrimoniales. Les caractéristiques du consentement sont renforcées ce qui apparemment confère une plus grande protection à la personne concernée. Il s'agit d'une « *manifestation de volonté, libre, spécifique, éclairée, univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que les données à caractère personnel la concernant, fassent l'objet d'un traitement* »[113]. Même lorsqu'aux termes de la loi française, le consentement « *spécifique* »[114], « *éclairé et exprès* »[115] pouvant «*résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle* »[116] est délivré, le contrôle s'entend également de la possibilité de retirer ce consentement sans aucun préjudice en résultant[117]. La liberté de

[110] M.-A. FRISON-ROCHE, « Le droit de la compliance », *D*. 2016, p.1871.
[111] V. sur cette question, A. DEBET, *op.cit.*
[112] Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[113] RGPD, art. 4.
[114] Loi informatique et libertés, art. 85.
[115] Loi informatique et libertés, art. 75.
[116] Loi informatique et libertés, art. 82.
[117] RGPD, art. 7.

choix est réellement mise en perspective par le dispositif à condition que l'utilisateur ait les moyens de l'exercer.

C'est d'ailleurs le constat opéré par la CNIL dans le cadre de sa délibération de janvier 2019, en retenant que même si l'utilisateur peut paramétrer son compte, le consentement recueilli n'est ni spécifique, ni univoque. La personne concernée doit faire la démarche de cliquer sur « *plus d'options* » pour accéder au paramétrage, mais en outre l'affichage d'annonces personnalisées est pré-coché par défaut, ce qui ne constitue pas un acte positif. Enfin, l'utilisateur est invité à cocher des cases visant à accepter des conditions générales d'utilisation et l'utilisation de ses informations par la plateforme, avant de pouvoir créer son compte. Le fait est qu'il y consent en bloc pour l'ensemble des finalités poursuivis. Le paragraphe 2 de l'article 7 RGPD précise à ce titre, que la demande de consentement doit faire l'objet d'un formalisme qui la distingue des autres informations délivrées à l'utilisateur de manière à ce qu'il n'y ait aucune confusion sur la portée du consentement. L'article 6 RGPD dispose, dans le prolongement, que le consentement doit être délivré pour chaque finalité à défaut de quoi sa validité est entachée. Cette exigence suppose en l'espèce, que le responsable du traitement fasse preuve d'une grande clarté pour afficher les finalités poursuivies. Reste que le risque de détournement de la finalité de la collecte est patent[118]. Cependant, la finalité ultime n'est pas toujours en rapport avec la finalité initiale, du fait de l'amas progressif de données. Le responsable de traitement ne peut anticiper l'ensemble des effets du traitement lorsqu'il le met en œuvre, « *même les entreprises les mieux intentionnées ne savent pas tout ce qui se passe avec les données qu'elles collectent* »[119]. Il en résulte que le consentement n'est pas spécifique et ne permet pas à la personne concernée de prendre conscience de l'étendue des traitements. En outre, les responsables de traitement doivent être en mesure de démontrer que les contrats proposés portant sur des équipements ou des services ne font pas obstacle au consentement de l'utilisateur final (l'article 34 de la loi informatique et libertés modifiée). Ce qui signifie qu'ils ne peuvent restreindre sans motif légitime, la configuration initiale du terminal de

[118] V. annexe.
[119] CNIL, *La forme des choix : données personnelles, design et frictions désirables*, préc., p.30.

l'utilisateur et notamment les conditions générales d'utilisation du service[120]. Ce dispositif interroge sur le rôle des acteurs dans la détermination du consentement et du niveau d'information nécessaire au regard de « motifs légitimes ». En cela le texte n'est pas abouti, produisant un effet inverse qui se traduit par un abaissement du niveau de protection de l'utilisateur. En l'état, la transparence est un vœu pieux mais sa reconnaissance pourrait restaurer la confiance dans le dispositif.

Pour la CNIL, les manquements commis par *Google* revêtent une particulière gravité. Même si la plateforme avait pu mettre en œuvre certains dispositifs en proposant de la documentation et des outils de paramétrage, cela n'a pas permis d'atténuer les manquements constatés, privant les utilisateurs de garanties fondamentales relatives aux traitements qui mettent en exergue des pans entiers de leur vie privée, en ce qu'ils reposent sur un volume considérable de données, une grande variété de services et des possibilités de combinaison de données quasi-illimitées. Les utilisateurs doivent conserver, *a fortiori* dans le cadre de ces traitements massifs, la maîtrise de leurs données. Ces manquements continus sont exacerbés du fait de la place prépondérante du système d'exploitation *Android* sur le marché français et de son modèle économique. La transparence résultant de l'accès à l'information et de sa contribution au processus décisionnel, est une condition nécessaire à la validité du consentement[121]. La transparence ne suffit pas à légitimer le traitement de données à caractère personnel mais conditionne la validité du consentement au moment de sa demande. Il appartient au responsable du traitement, aux termes de l'article 7 RGPD, de prouver à tout moment la manifestation du consentement de l'utilisateur. Il assume la charge de la preuve dans la logique du principe d'*accountability*.

La capacité à consentir. En matière de données personnelles, les règles relatives à la capacité à consentir ne sont pas précisées, sauf en ce qui concerne l'âge ou la contrainte. Ces critères doivent par ailleurs être appréhendés selon une même logique, sous l'angle du discernement. Or, l'absence de discernement n'est pas autre chose qu'une forme de contrainte dans la prise de décision qui s'impose à l'individu. Certes, le fait de fixer

[120] X. D., « Loi relative à la protection des données personnelles : aspects contractuels », *AJ Contrats*, 2018, p.301.
[121] TGI Paris, 7 août 2018, Twitter, n°14/07300.

objectivement un âge pour déterminer la capacité à consentir a pour seul effet de garantir une forme de sécurité juridique et d'éviter que l'ensemble du raisonnement repose sur le critère subjectif du discernement. La capacité de consentir ne s'arrête pas à la question de l'âge, elle renvoie aux règles du code civil qui viennent se superposer logiquement à celles relatives aux données à caractère personnel[122]. Cette interaction avec d'autres instruments législatifs n'est pas une spécificité nationale mais se conçoit également à l'échelon européen ce qui, d'une certaine manière relève du bon sens ; la législation sur les données n'a pas pour ambition de régler les questions de procédure.

La question de l'âge. Cette question est récurrente et tout particulièrement en matière de comportement à caractère sexuel[123]. Elle a été débattue dans le cadre de la loi n°2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes. L'article 2 portant sur le consentement d'un mineur de 15 ans à une relation sexuelle avec un majeur appelle à commentaire. Par-delà l'âge auquel il peut consentir à la relation sexuelle sans que l'on puisse invoquer la violence, la menace, la contrainte ou la surprise, éléments matérialisant le viol au sens de l'article 222-23 du code pénal, il conviendra d'apprécier *in concreto* la maturité ou le discernement du mineur de 15 ans pour évaluer son niveau de compréhension et sa capacité à prendre le recul nécessaire pour éviter toute confusion. Autrement dit, la seule référence à l'âge du mineur ne suffit plus à évaluer sa maturité ou son discernement[124]. C'est un élément d'objectivation du consentement. La représentation pornographique est un exemple intéressant de ce point de vue[125]. Certes, la représentation pornographique susceptible d'être vue par un mineur est pénalement prohibée. Donc, la majorité civile reste le critère requis. Cependant, même à 18 ans, les adultes doivent consentir à recevoir de tels contenus. Or, ce qui caractérise désormais les contenus pornographiques, c'est

[122] Article 70 de la loi informatique et libertés : « *Sont destinataires de l'information et exercent les droits de la personne concernée par le traitement les titulaires de l'exercice de l'autorité parentale, pour les mineurs, ou la personne chargée d'une mission de représentation dans le cadre d'une tutelle, d'une habilitation familiale ou d'un mandat de protection future, pour les majeurs protégés dont l'état ne leur permet pas de prendre seuls une décision personnelle éclairée*. »

[123] M. SWEENEY, M. TOUZEIL-DIVINA, *Droit(s) aux(x) Sexe(s)*, Editions de l'Épitoge, l'Unité du Droit, mars 2017.

[124] J. LÉONHARD, « Projet de loi renforçant la lutte contre les violences sexuelles : quel avenir pour l'article 2 ? », http://blog.leclubdesjuristes.com/projet-de-loi-renforcant-la-lutte-contre-les-violences-sexuelles-quel-avenir-pour-larticle-2/, vu le 25 mai 2018.

[125] « *La pornographie est un plaisir inoffensif si on ne la prend pas au sérieux et si l'on ne croit pas qu'elle corresponde à la vraie vie. Quiconque la confond avec la réalité sera gravement déçu », in The little red school book, v. CEDH, 7 décembre 1976, Handyside,* aff. n°5493/72.

qu'ils sont mis à disposition du public sans que ce dernier n'y consente nécessairement, y compris les adultes. Par ailleurs, qu'un enfant ait en moyenne 11, 12 ou 13 ans, voire davantage lorsqu'il est exposé pour la première fois à des contenus pornographiques en ligne, n'est pas un critère déterminant pour l'analyse. Se pose la question de savoir quel est le « bon âge » pour être exposé à la pornographie. Les anciens modèles de communication considèrent que l'âge de la majorité reste fixé à 18 ans pour l'accès aux contenus pornographiques, mais ce critère ne correspond pas à la maturité cérébrale et peut avoir un impact sur le développement de l'individu. L'adulte peut être heurté par de tels contenus lorsqu'il les a ou non sollicités car c'est son désir de les recevoir qui est questionné, de même que sa capacité à prendre de la distance avec les contenus eux-mêmes en considérant qu'ils ne sont, au final, qu'une représentation de la réalité.

La majorité numérique questionnée. L'âge de la majorité numérique a été âprement discuté dans le cadre de la réforme de la loi emblématique Informatique et liberté dans le cadre des marges de manœuvre laissées à la discrétion des États à la lecture du RGPD. Il s'agit donc pour les États de définir un âge entre 13 et 16 ans permettant au mineur concerné de consentir à l'utilisation de ses données[126], conditionnant l'application de l'article 17 du RGPD, et spécifié par la loi n°2016-1321 du 7 octobre 2016 pour une République numérique relatif au droit à l'oubli des mineurs. Les députés et sénateurs se sont opposés sur ce point pour fixer à 15 ou 16 ans l'âge requis, mais sont allés au-delà des marges de manœuvre en fixant le cadre dans lequel le consentement doit être délivré [127] . Par analogie, on peut alors imaginer que ce mineur qui dispose de la maturité suffisante pour consentir à l'utilisation de ses données, pourrait également consentir l'accès à certains contenus.

[126] RGPD, art. 8 : *1. Lorsque l'article 6, paragraphe 1, point a), s'applique, en ce qui concerne l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant. Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans.*
2. Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles.
3. Le paragraphe 1 ne porte pas atteinte au droit général des contrats des États membres, notamment aux règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant.
[127] Cons. Const., n°2018-765 DC du 12 juin 2018, Loi relative à la protection des données à caractère personnel.

Pour autant, la détermination de l'âge requis est secondaire, car les données de mineurs, sont largement exploitées, tout d'abord par leurs parents et ce, dès leur plus jeune âge, pour les protéger, les surveiller, les médicaliser, les socialiser, etc. mais ensuite par les opérateurs dans le cadre des réseaux sociaux, moteurs de recherches et autres plateformes de commerce électronique, dans une perspective commerciale. Le manque à gagner résultant de ce choix est loin d'être anodin car en fonction de l'âge, le consentement est délivré par les parents, ou représentants légaux, et non par le mineur, qui reste la cible visée par les opérateurs. D'une certaine manière en fixant à 15 ans la majorité numérique[128], la France s'est positionnée en demi-teinte par rapport aux autres États ayant majoritairement adopté le seuil de 13 ou 14 ans, sans réalisme au regard des usages des mineurs sur les réseaux sociaux, la faiblesse des contrôles parentaux ou l'intérêt des opérateurs. Ces derniers doivent réaliser en pratique des opérations complexes et algorithmiques pour déterminer quelles personnes concernées peuvent bénéficier des emailings dans quels pays, etc[129]. Pour autant c'est la volonté de s'aligner sur l'âge de la majorité sexuelle qui a motivé les députés, ce qui reste somme toute, très discutable, dans la mesure où la contrainte ne disparaît pas du fait de l'acquisition d'une maturité supposée[130]. Dès lors la démarche adoptée à l'échelle européenne n'offre pas de nouveaux éléments structurants pour réfléchir utilement au rapport entre l'âge et l'acquisition du consentement. Bien au contraire, le RGPD et la loi française du 20 juin 2018 reformulée par l'ordonnance du 12 décembre 2018 apportent leur lot de questions nouvelles qui aboutissent à obscurcir les effets de cette majorité numérique, et notamment le rapport des mineurs à leurs représentants légaux.

Le consentement des mineurs versus le consentement des représentants légaux. Les données des mineurs sont particulièrement convoitées pour de multiples raisons que l'on identifie aisément. Elles sont gérées lors de la

[128] Voir, B. CHARRIER, « Le consentement exprimé par les mineurs en ligne », *Dalloz IP/IT* 2018, p.333.

[129] K. LOBRY, « Le consentement des mineurs sur internet : une vraie problématique pour les entreprises », 29 octobre 2018, https://dpo-consulting.fr/

[130] Le considérant 38 RGPD précise que les mineurs « *méritent une protection spécifique […] parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel* », notamment à l'égard des traitements des données « *à des fins de marketing ou de création de profils de personnalité ou d'utilisateur* » et intervenant lors de l'utilisation de services proposés directement aux mineurs.

minorité numérique (entre 13 et 15 ans en l'espèce), conjointement par le mineur concerné et les titulaires de l'autorité parentale[131]. Il s'agit donc d'associer le mineur aux décisions le concernant, laissant croire à son autonomie, mais il convient de ne pas oublier qu'il appartient aux représentants légaux d'autoriser le traitement des données collectées par les services en ligne (dénommés services de la société de l'information au sein du RGPD[132]). Encore faut-il que les parents assument le dispositif et que les mineurs soient honnêtes sur leur âge lors de l'utilisation des réseaux, notamment. C'est bien toute la difficulté du consentement lorsque les mineurs utilisent les services en ligne avant leurs 13 ans, d'où la nécessité de s'assurer que le consentement a bien été délivré par le titulaire de l'autorité parentale ou conjointement si nécessaire. Le responsable de traitement se retrouve face à une difficulté relative à la vérification de l'identité du représentant légal. A travers un formulaire en ligne, il est impossible d'avoir la certitude que les informations nécessaires ont bien été délivrées par le représentant légal. On peut imaginer que les responsables de traitement programment l'envoi d'un email automatique pour chaque formulaire dont la rubrique dédiée au représentant légal a été complétée afin d'obtenir une confirmation de leur part[133], ce qui permettrait d'instaurer une véritable confiance familiale !

Reste qu'en cas d'opposition entre le mineur et les représentants légaux, la majorité numérique ne permet pas au mineur de faire prévaloir sa volonté tant qu'il n'a pas atteint ses 18 ans, sauf en matière de données de santé en vertu de l'article 70 de la loi informatique et libertés. Mais l'effectivité du dispositif reste à démontrer et en appelle à une démarche plus souple *a priori* impliquant les autorités de régulation dans la réflexion fonctionnelle de la mise en œuvre des intérêts de l'enfant, et ce, de manière casuiste. Car selon les cas, l'utilisation des services en ligne fait partie intégrante de son éducation et de sa scolarité. Dès lors, le mineur n'a nullement besoin de consentir car il agit sous la responsabilité de l'équipe pédagogique. Dans d'autres cas, il agit sous l'autorité de ses représentants légaux sans que ces derniers soient en capacité d'évaluer les enjeux du consentement. Enfin, le mineur agit dans son cercle

[131] RGPD, art. 8.

[132] RGPD, art. 4 § 25 du, CJUE, 2 décembre 2010, aff. C-108/09, Ker Optika ; ces services couvrent les contrats et autres services conclus ou transmis en ligne.

[133] K. LOBRY, « Le consentement des mineurs sur internet : une vraie problématique pour les entreprises », préc.

d'amis, et se passe du consentement des représentants légaux. En tout état de cause, il existe des risques qui impactent la construction de sa « personnalité numérique » en anticipant la construction de la « bulle numérique » sans le consentement des parties prenantes.

Le recours à la dignité ? Si l'atteinte à la dignité de la personne non consentante constitue un rempart attendu à de telles pratiques, «*(étant) susceptible de tout recouvrir* »[134], il convient de manier ce principe fondamental avec précaution car il pourrait venir en renfort tout à la fois pour justifier, réglementer ou interdire la pornographie[135], la liberté d'expression[136], le traitement de données personnelles[137].

La dignité n'est pas définie[138] et elle est largement revendiquée et appréciée, notamment par le juge européen[139], comme « *un fondement général sur lequel peut s'entendre démocratiquement et juridiquement la globalité (des) membres (de la société) – quelquefois au prix de lourdes ambiguïtés* ».[140] Dès lors ce principe fondamental de dignité prend les traits d'un véritable principe matriciel. De manière à garantir la sécurité juridique, il est préférable de se référer aux droits qui se rapportent à ce principe, et de s'en tenir au consentement[141]. Ce consentement pourrait revêtir une signification s'il était accompagné d'une mise en pouvoir d'agir des utilisateurs. Ce n'est donc qu'en

---

[134] E. PICARD, « L'émergence des droits fondamentaux en France », *AJDA*, 1998, p.6 et s.

[135] L'article L. 211-1 du code du cinéma et de l'image animée dispose que : « *La représentation cinématographique est subordonnée à l'obtention d'un visa d'exploitation délivré par le ministre chargé de la culture. / Ce visa peut être refusé ou sa délivrance subordonnée à des conditions pour des motifs tirés de la protection de l'enfance et de la jeunesse ou du respect de la dignité humaine* (...) « ; Voir pour illustration, CE, 13 janvier 2017, Association Promouvoir, req. n°397819 ; CE, 5 avril 2019, salafistes, req. 417343.

[136] CE, Ord., 9 janvier 2014, Ministre de l'intérieur c/ Société Les Productions de la Plume et M. Dieudonné M'Bala M'Bala, req. n°374508.

[137] Convention 108 modernisée du Conseil de l'Europe CM/inf (2018)15-final, pour la protection des personnes à l'égard du traitement des données à caractère personnel, 18 mai 2018, intègre la nécessité de « *garantir la dignité humaine ainsi que la protection des droits de l'Homme et des libertés fondamentales de toute personne, et, eu égard à la diversification, à l'intensification et à la mondialisation des traitements des données et des flux de données à caractère personnel, l'autonomie personnelle, fondée sur le droit de la personne de contrôler ses propres données à caractère personnel et le traitement qui en est fait* ».

[138] V. CHAMPEIL-DESPLATS, « Dignité de la personne humaine : peut-on parler d'une exception française ? », Les Cahiers de l'Institut Louis Favoreu, PUAM, 2013, *Existe-il une exception française en matière de droits fondamentaux?*, p.173 et s. ; X. BIOY, « Rapport introductif. Le concept de dignité », in L. BURGORGUE-LARSEN (dir.), *La dignité saisie par les juges en Europe*, Bruylant, *Droit et Justice*, n° 95, 2010, p. 13 et s.

[139] C. GREWE, « La dignité humaine dans la jurisprudence de la CEDH », *Revue Générale du droit*, novembre 2014, http://www.revuegeneraledudroit.eu/blog/2014/11/06/la-dignite-humaine-dans-la-jurisprudence-de-la-cour-europeenne-des-droits-de-lhomme/

[140] *Idem.*

[141] CEDH, 17 février 2005, K.A et A.D. c/ Belgique, aff. 42758/98 ; 45558/99.

l'absence de consentement que l'atteinte à la dignité « pourrait » être retenue, et non en première intention. L'absence de consentement pourrait caractériser une atteinte à la dignité. Le juge français affiche pourtant une conception « paternaliste » qui privilégie dans certains cas, la protection de l'individu contre lui-même, niant le consentement, comme ce fut le cas dans l'emblématique affaire du « lancer de nains »[142]. La prudence est alors de mise car le principe de dignité, pour constituer un fondement juridique solide, doit afficher une ligne directrice l'éloignant d'une appréciation casuistique par le juge, sous peine de subjectiviser de trop la protection des droits fondamentaux. Par exemple, la protection des mineurs est efficace seulement s'ils apprennent dès leur plus jeune âge à coder la donnée, la manier, et comprendre le fonctionnement des *big data*. Outre la question de l'autonomie personnelle, il s'agit de garantir l'autonomie de la protection des données personnelles au regard de la dignité pour limiter les effets d'une protection de l'individu contre lui-même qui aurait pour effet de diluer les responsabilités. Un raisonnement similaire pourrait être tenu en matière d'accès à des messages pornographiques, ou d'atteinte à la liberté d'expression sous peine de voir réapparaître un ordre moral par trop subjectif et entraînant la déresponsabilisation des acteurs.

Annexe

Délibération n°SAN-2019-001 du 21 janvier 2019

Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Jean-François CARREZ, Président, M. Alexandre LINDEN, Vice-président, Mme Dominique CASTERA, Mme Marie-Hélène MITJAVILE et M. Maurice RONAI, membres ;

[142] CE, 27 octobre 1995, Commune de Morsang-sur-Orge et Ville d'Aix en Provence, *RFDA*, 1995, p.1204, concl. sur P. FRYDMAN ; V. sur ce raisonnement, V. CHAMPEIL-DESPLATS, préc. ; D. ROMAN, « A corps défendant : la protection de l'individu contre lui-même », *D.*, 2007, chr. p.1284.

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 45 et suivants ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi
n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2018-199C du 20 septembre 2018 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification de tout traitement relatif à l'utilisation du système d'exploitation Android pour mobile multifonction incluant la création d'un compte Google ;

Vu la décision de la Présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 2 octobre 2018 ;

Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, du 22 octobre 2018 ;

Vu les observations écrites versées par la société Google LLC. le 22 novembre 2018 ;

Vu les observations en réponse du commissaire rapporteur du 7 décembre 2018 ;

Vu les observations en réponse versées par la société Google LLC. le 4 janvier 2019 ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 15 janvier 2019 :

M. François PELLEGRINI, commissaire, entendu en son rapport ;

En qualité de représentants de la société Google LLC. :

En qualité de conseils de la société Google LLC. ;

[…]

Mme Eve JULLIEN, commissaire du Gouvernement, n'ayant pas formulé d'observation ;

La société ayant eu la parole en dernier ;

Après en avoir délibéré, a adopté la décision suivante :

Faits et procédure

Fondée en 1998, la société Google LLC. (ci-après Google ou la société) est une société à responsabilité limitée de droit américain dont le siège social est situé à Moutain View, en Californie (Etats-Unis).

Filiale à 100% de la société ALPHABET depuis 2015, la société a réalisé un chiffre d'affaires de 109,7 milliards de dollars (soit environ 96 milliards d'euros) en 2017. Elle possède plus de 70 bureaux implantés dans une cinquantaine de pays et compte environ 70 000 salariés à travers le monde. En France, elle dispose d'un établissement, la société Google France Sarl, située 8 rue de Londres à Paris (75009), qui compte environ 600 salariés et a réalisé un chiffre d'affaires d'environ 325 millions d'euros en 2017.

Depuis qu'elle existe, la société a développé une pluralité de services à destination des entreprises et des particuliers (ex : le service de messagerie Gmail, le moteur de recherche Google Search, YouTube etc.). Elle a également conçu le système d'exploitation pour les terminaux mobiles Android qui comprend le magasin d'applications Google Play. La société exerce en outre une activité de régie publicitaire.

En 2016, ce système d'exploitation comptait 27 millions d'utilisateurs en France.

Les 25 et 28 mai 2018, la Commission nationale de l'informatique et des libertés (ci-après CNIL ou la Commission) a été saisie de deux plaintes collectives déposées en application de l'article 80 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (Règlement général sur la protection des données, ci-après RGPD ou le Règlement) respectivement par l'association None Of Your Business (ci-

après NOYB) et l'association La Quadrature du Net (ci-après LQDN). De manière cumulée, ces plaintes regroupent les réclamations de 9974 personnes.

Dans sa plainte, l'association NOYB indique notamment que les utilisateurs de terminaux mobiles Android sont tenus d'accepter la politique de confidentialité et les conditions générales d'utilisation des services de Google et qu'à défaut d'une telle acceptation, ils ne pourraient utiliser leur terminal.

L'association LQDN estime quant à elle, qu'indépendamment du terminal utilisé, Google ne dispose pas de bases juridiques valables pour mettre en œuvre les traitements de données à caractère personnel à des fins d'analyse comportementale et de ciblage publicitaire.

Le 1er juin 2018, la CNIL a soumis les plaintes précitées à ses homologues européens via le système européen d'échange d'information en vue de la désignation d'une éventuelle autorité chef de file conformément aux dispositions de l'article 56 du RGPD.

En application de la décision n° 2018-199C du 20 septembre 2018 de la Présidente de la Commission, un contrôle en ligne a été effectué le 21 septembre suivant afin de vérifier la conformité de tout traitement relatif à l'utilisation du système d'exploitation Android pour équipement mobile, incluant la création d'un compte Google, à la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après loi Informatique et Libertés ou loi du 6 janvier 1978) et au RGPD.

Le procès-verbal de contrôle en ligne n° 2018-199/1 a été notifié aux sociétés GOOGLE LLC. et Google France SARL les 24 et 25 septembre 2018.

Les deux sociétés ont également eu communication des plaintes susmentionnées par courriers de la CNIL le 28 septembre 2018.

Aux fins d'instruction de ces éléments, la Présidente de la CNIL a désigné, le 2 octobre 2018, M. François PELLEGRINI en qualité de rapporteur sur le fondement de l'article 47 de la loi du 6 janvier 1978.

A l'issue de son instruction, le rapporteur a fait notifier aux sociétés Google LLC. et Google France SARL, le 22 octobre 2018, un rapport détaillant des manquements relatifs aux articles 6, 12 et 13 du RGPD qu'il estimait constitués en l'espèce.

Ce rapport proposait à la formation restreinte de la CNIL de prononcer à l'encontre de la société Google LLC. une sanction pécuniaire de 50 millions d'euros, rendue publique. Il était également proposé son insertion dans une publication, journal ou support que la formation restreinte désignerait.

Etait également jointe au rapport une convocation à la séance de la formation restreinte du 10 janvier 2019. L'organisme disposait d'un délai d'un mois pour communiquer ses observations écrites.

Par lettre du 7 novembre 2018, la société a demandé une audition au rapporteur, à laquelle il n'a pas été fait droit par courrier du 13 novembre 2018. A la même date, la société a également formulé une demande de huis clos et de report de séance, à laquelle il n'a pas été fait droit, par courrier du 15 novembre 2018.

Le 22 novembre 2018, la société a produit des observations écrites sur le rapport. Ces observations ont fait l'objet d'une réponse du rapporteur le 7 décembre 2018.

Par lettre du 11 décembre 2018, la société, qui disposait de quinze jours à compter de la réception de la réponse du rapporteur, a sollicité de la part du Président de la formation restreinte le report de la séance ainsi qu'une extension du délai pour produire ses nouvelles observations. La demande a été acceptée par le Président de la formation restreinte le 13 décembre 2018, qui a décidé, d'une part, de repousser de deux semaines - jusqu'au 7 janvier - le délai de production de ces observations et, d'autre part, de reporter la séance au 15 janvier 2019.

Le 4 janvier 2019, la société a produit de nouvelles observations en réponse à celles du rapporteur.

L'ensemble des observations a été réitéré oralement par la société et le rapporteur lors de la séance de la formation restreinte du 15 janvier 2019.

II. Motifs de la décision

1. Sur la compétence de la CNIL

L'article 55 paragraphe 1 du RGPD dispose : Chaque autorité de contrôle est compétente pour exercer les missions et les pouvoirs dont elle est investie conformément au présent règlement sur le territoire de l'État membre dont elle relève.

L'article 56 paragraphe 1 du RGPD dispose : Sans préjudice de l'article 55, l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant, conformément à la procédure prévue à l'article 60.

La société soutient tout d'abord que la CNIL n'est pas compétente pour mener cette procédure et qu'elle aurait dû transmettre les plaintes reçues à l'autorité de protection des données irlandaise (Data Protection Commission, ci-après DPC) à laquelle il appartiendrait, en tant qu'autorité chef de file de Google, de traiter ces plaintes portant sur des traitements transfrontaliers, et ce conformément à la procédure de coopération établie à l'article 60 du RGPD. La société considère en effet que la société Google Ireland Limited doit être considérée comme son établissement principal au sein de l'Union européenne pour certains des traitements transfrontaliers qu'elle met en œuvre, et notamment ceux objets des plaintes reçues par la CNIL. Par conséquent, l'autorité de protection des données devrait selon elle être regardée comme son autorité de contrôle chef de file et être chargée, à ce titre, de traiter les plaintes reçues par la CNIL.

Pour attester du fait que la société Google Ireland Limited constitue son établissement principal au sein de l'Union, elle précise que cette société est le siège social de Google pour ses opérations européennes depuis 2003 et qu'elle est l'entité en charge de plusieurs fonctions organisationnelles nécessaires à la réalisation de ces opérations pour la zone Europe, Moyen-Orient et Afrique (secrétariat général, fiscalité, comptabilité, audit interne, etc.). Elle indique également que la conclusion de l'intégralité des contrats de vente de publicités avec les clients basés dans l'Union européenne relève de cette société. Cette société emploie plus de 3 600 salariés et dispose, entre autres, d'une équipe dédiée en charge de la gestion des demandes faites au sein de l'Union européenne en lien avec la confidentialité et d'un responsable chargé de la protection de la vie privée. Elle précise enfin qu'une réorganisation tant opérationnelle qu'organisationnelle est en cours en vue de faire de la société Google Ireland Limited le responsable de traitement pour certains traitements de données à caractère personnel concernant les ressortissants européens.

Elle considère également que la définition d'établissement principal doit être distinguée de celle de responsable de traitement et que si le législateur européen avait voulu que la notion d'établissement principal soit interprétée comme le lieu où les décisions concernant les traitements sont prises, il l'aurait expressément indiqué.

Elle considère ensuite que, compte tenu de la nature transfrontalière des traitements de personnalisation de la publicité, du nombre significatif d'utilisateurs d'Android en Europe et des questions soulevées en lien avec ces traitements, les mécanismes de coopération et de cohérence tels que prévus aux articles 60, 64 et 65 du RGPD auraient dû s'appliquer. Elle précise notamment que le Comité européen de

la protection des données (ci-après CEPD) aurait dû être saisi en cas de doute sur la détermination de l'autorité chef de file.

Enfin, la société estime que les discussions informelles qui ont pu avoir lieu entre les autres autorités européennes de contrôle sur cette procédure sont sans effet juridique dès lors qu'elles ont eu lieu sans sa présence.

Sur la qualité d'établissement principal de la société Google Ireland Limited

L'article 4 (16) du RGPD définit la notion d'établissement principal de la manière suivante : a) en ce qui concerne un responsable du traitement établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel soient prises dans un autre établissement du responsable du traitement dans l'Union et que ce dernier établissement a le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal .

Le considérant 36 du RGPD précise quant à lui : L'établissement principal d'un responsable du traitement dans l'Union devrait être déterminé en fonction de critères objectifs et devrait supposer l'exercice effectif et réel d'activités de gestion déterminant les décisions principales quant aux finalités et aux moyens du traitement dans le cadre d'un dispositif stable.

La formation restreinte considère qu'il résulte de ces dispositions que, pour pouvoir être qualifié d'établissement principal, l'établissement concerné doit disposer d'un pouvoir de décision vis-à-vis des traitements de données à caractère personnel en cause. La qualité d'établissement principal suppose en effet l'exercice effectif et réel d'activités de gestion déterminant les décisions principales quant aux finalités et aux moyens du traitement.

Dès lors, l'existence d'un établissement principal s'apprécie *in concreto*, au regard de critères objectifs, et l'établissement principal ne saurait correspondre automatiquement au siège social du responsable de traitement en Europe.

La formation restreinte relève que cette analyse est également celle retenue par l'ensemble des autorités européennes de contrôle, comme en attestent les lignes directrices du CEPD du 5 avril 2017 concernant la désignation d'une autorité de contrôle chef de file d'un responsable de traitement ou d'un sous-traitant (WP244). Ces dernières indiquent que : l'administration centrale est le lieu où sont prises les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel, et ce lieu a le pouvoir de faire appliquer ces décisions .

La formation restreinte relève en outre que ces mêmes lignes directrices indiquent que : Le règlement général n'autorise pas l'élection de juridiction (forum shopping)(…). Les conclusions ne peuvent reposer exclusivement sur des déclarations de l'organisation considérée.

Il convient ainsi d'apprécier les pouvoirs décisionnels dont dispose la société Google Ireland Limited pour déterminer si elle peut être qualifiée d'établissement principal.

A cet égard, la formation restreinte relève que la société Google Ireland Limited dispose certes de nombreux moyens financiers et humains qui permettent la fourniture effective de services par Google en Europe, notamment par le biais de la vente de prestations publicitaires.

Toutefois, si ces éléments attestent de cette participation, la formation restreinte considère qu'ils ne permettent pas d'emporter la qualification de la société Google Ireland Limited en tant qu'établissement principal. Les éléments fournis ne démontrent pas par eux-mêmes que la société Google Ireland Limited aurait disposé, à la date d'engagement des poursuites, d'un quelconque pouvoir décisionnel quant aux finalités et aux moyens des traitements couverts par la politique de confidentialité présentée à l'utilisateur lors de la création de son compte, à l'occasion de la configuration de son téléphone mobile sous Android. Ces éléments révèlent seulement l'implication de cette entité dans le cadre de différentes activités de la société (activités financières et comptables, vente d'espaces publicitaires, passation de contrats etc.).

La formation restreinte relève par ailleurs que la société Google Ireland Limited n'est pas mentionnée dans les Règles de confidentialité de la société en date du 25 mai 2018 comme étant l'entité où sont prises les décisions principales quant aux finalités et aux moyens des traitements couverts par la politique de confidentialité présentée à l'utilisateur lors de la création de son compte, à l'occasion de la configuration de son téléphone mobile sous Android.

Elle souligne également que la société Google Ireland Limited n'a pas désigné de délégué à la protection des données qui serait en charge des traitements de données à caractère personnel qu'elle pourrait mettre en œuvre dans l'Union européenne. Elle relève en outre que le système d'exploitation Android est développé uniquement par la société Google LLC.

Enfin, la formation restreinte relève que la société a elle-même indiqué, par courrier en date du 3 décembre 2018 adressé à la DPC, que le transfert de

responsabilité de Google LLC. vers la société Google Ireland Limited sur certains traitements de données à caractère personnel concernant les ressortissants européens serait finalisé le 31 janvier 2019. Elle a ultérieurement précisé procéder à la mise à jour de ses règles de confidentialité qui entreront en application le 22 janvier 2019.

Au vu de l'ensemble de ces éléments, la formation restreinte considère que la société Google Ireland Limited ne peut être considérée comme l'établissement principal de la société Google LLC. en Europe au sens de l'article 4 (16) du RGPD, dès lors qu'il n'est pas établi qu'elle dispose d'un pouvoir décisionnel quant aux traitements couverts par la politique de confidentialité présentée à l'utilisateur lors de la création de son compte à l'occasion de la configuration de son téléphone mobile sous Android.

En l'absence d'établissement principal permettant l'identification d'une autorité chef de file, la CNIL était compétente pour engager cette procédure et pour exercer l'ensemble de ses pouvoirs au titre de l'article 58 du RGPD.

b) Sur l'application des procédures de coopération et de cohérence

En premier lieu, la société soutient que la CNIL aurait dû saisir le CEPD en raison de l'incertitude quant à l'identification de l'autorité de contrôle devant agir en qualité d'autorité chef de file.

La formation restreinte considère tout d'abord que l'absence d'établissement principal d'un responsable de traitement au sein de l'Union européenne n'engendre pas par elle-même d'incertitude sur l'identification d'une autorité de contrôle pouvant agir en qualité d'autorité chef de file. Il résulte seulement de cette absence d'établissement principal que l'identification d'une autorité chef de file n'a pas lieu d'être, et que le mécanisme de guichet unique n'a pas vocation à s'appliquer.

La formation restreinte relève ensuite que la CNIL a immédiatement communiqué les réclamations reçues à l'ensemble des autorités de contrôle, via le système européen d'échange d'information, en vue de l'identification d'une éventuelle autorité chef de file, conformément aux dispositions de l'article 56 du RGPD.

La formation restreinte note que, dans le cadre de cette procédure, aucune autorité de contrôle, ni le Président du Comité, n'ont jugé nécessaire de saisir le CEPD en raison d'incertitudes sur l'identification de l'autorité chef de file ou la compétence de la CNIL.

Elle observe en outre que l'analyse concluant à l'absence d'établissement principal de la société Google LLC. en Europe pour les traitements visés par les plaintes, et l'absence d'autorité chef de file qui en résulte, était partagée par la DPC.

Elle relève ainsi que la DPC a publiquement affirmé le 27 août 2018 - dans un article de presse de l'Irish Times - qu'elle n'était pas l'autorité chef de file pour les traitements qui pouvaient être mis en œuvre par la société : la Commission de protection des données n'est pas le "principal régulateur" de Google (ni, en termes de protection des données, son "autorité de contrôle chef de file") [...] Google LLC, société américaine, est le responsable de traitement et Google ne peut absolument pas se prévaloir du mécanisme de guichet unique. […]. La position actuelle est que Google est soumis au contrôle de toutes les autorités de contrôle européennes […] .

Il ne résulte dès lors pas de l'instruction qu'il aurait existé des doutes ou des points de vue divergents au sein des autorités de contrôle de nature à imposer une saisine du CEPD, conformément à l'article 65 du RGPD. Par ailleurs, compte tenu des lignes directrices déjà adoptées au niveau européen pour guider les autorités nationales dans l'identification de l'éventuelle autorité chef de file, il n'existait pas de question nouvelle justifiant la saisine du CEPD par la CNIL en application de l'article 64.

Compte tenu de l'ensemble de ces éléments, la formation restreinte considère que la CNIL n'était pas tenue de saisir le CEPD en vue de l'identification d'une autorité chef de file.

En second lieu, si la société soutient que la CNIL aurait dû coopérer sur l'instruction des plaintes et les suites qu'il convenait de leur apporter, la formation restreinte rappelle, ainsi qu'il a été dit précédemment, que la CNIL a communiqué, dès leur réception, les réclamations à l'ensemble des autorités de contrôle de l'Union européenne, via le système européen d'échange d'information, en vue de l'identification d'une éventuelle autorité chef de file.

La formation restreinte relève ainsi qu'une procédure de coopération a bien été engagée avec les autorités de contrôle, et ce conformément aux dispositions de l'article 56 du RGPD, dans un premier temps sur la seule question de l'identification des compétences respectives de ces autorités.

La formation restreinte observe que cette étape de diffusion d'information et de détermination d'une éventuelle autorité chef de file constitue un préalable à l'application éventuelle du mécanisme du guichet unique prévu à l'article 60 du RGPD.

La formation relève ensuite que cette démarche et les échanges qui en ont résulté n'ayant pas conduit à identifier un établissement principal ni, par suite, une autorité chef de file, aucune autre obligation de coopération ne s'imposait ultérieurement à la CNIL, notamment au titre de l'article 60 du RGPD.

La formation restreinte rappelle enfin que, dans un souci de cohérence, conformément aux orientations rappelées à l'article 63 du RGPD, la CNIL a informé et consulté ses homologues européens à plusieurs reprises sur les investigations qu'elle a menées, et tenu le plus grand compte des lignes directrices adoptées par le CEPD en vue d'assurer une application uniforme du règlement.

Compte tenu de ces éléments, la formation restreinte considère que les procédures de coopération et de cohérence n'ont pas été méconnues.

Au demeurant, la formation restreinte relève que sauf dispositions expresses, ce qui n'est pas le cas en l'espèce concernant la détermination de l'autorité chef de file, les autorités de contrôle ne sont pas tenues d'informer les responsables de traitement lors de la mise en œuvre d'actions de coopération ni de les mettre à même de participer aux échanges entre autorités.

2. Sur la procédure

En premier lieu, la société soutient que la recevabilité des plaintes déposées par les associations None Of Your Business et La Quadrature du Net n'est pas établie.

La formation restreinte considère la question de la recevabilité des plaintes précitées n'a en tout état de cause pas d'influence sur la légalité de la présente procédure, la saisine de la formation n'étant pas nécessairement subordonnée à la réception d'une plainte et pouvant résulter d'une auto-saisine de la Commission sur la base des constats opérés par les services de cette dernière. Elle rappelle que la CNIL a pour mission de contrôler l'application du règlement et de veiller au respect de celui-ci et qu'elle dispose, pour ce faire, du pouvoir d'effectuer des enquêtes, conformément à l'article 57 1. a) et h) du RGPD.

Au demeurant, la formation restreinte note que l'article 80 du RGPD prévoit la possibilité pour une personne de mandater une association à but non lucratif, qui a été valablement constitué[e] conformément au droit d'un État membre, dont les objectifs statutaires sont d'intérêt public et est acti[ve] dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel pour introduire une réclamation en leur nom.

S’agissant de LQDN, la formation restreinte relève qu’il s’agit d’une association française créée le 3 janvier 2013. Il ressort de ses statuts que cette association a notamment pour objet de mener des actions pour assurer la défense des droits et libertés fondamentaux dans l’espace numérique [...] .

S’agissant de NOYB, elle relève qu’il s’agit d’une association à but non lucratif valablement constituée sur le territoire autrichien depuis 12 juin 2017. Il ressort de ses statuts que son objet est notamment de représenter les droits et les intérêts des utilisateurs dans le domaine numérique (notamment les droits des consommateurs, les droits fondamentaux de la vie privée, la protection des données, la liberté d'expression, la liberté d'information et le droit fondamental à un recours effectif).

La formation relève également que ces deux associations ont reçu de la part des personnes les ayant saisies un mandat de représentation au titre de l’article 80 du RGPD.

En second lieu, la société fait valoir que la procédure engagée à son encontre a méconnu son droit à un procès équitable tel que prévu notamment à l’article 6 de la Convention de sauvegarde des droits de l’homme et des libertés fondamentales.

Sur ce point, elle soutient d’une part, que le rapport proposant une sanction ainsi que les réponses apportées par le rapporteur à ses observations lui ont été adressées uniquement en français et d’autre part, que le refus d’extension du délai qui lui été opposé pour produire ses premières observations a limité le temps dont elle disposait pour préparer sa défense. Elle estime également que le report de séance ainsi que le délai supplémentaire qui lui a finalement été accordé pour produire ses secondes observations n’étaient toujours pas suffisants.

La formation restreinte relève tout d’abord que la notification d’un rapport de sanction en langue française répond à l’obligation légale fixée à l’article 111-1 du code des relations entre le public et l’administration qui prévoit que L'usage de la langue française est prescrit dans les échanges entre le public et l'administration, conformément aux dispositions de la loi n° 94-665 du 4 aout 1994 relative à l'emploi de la langue française .

En outre, aucune disposition légale ou supra nationale n’impose à la CNIL de traduire les documents qu’elle produit.

Au demeurant, la société dispose d’un établissement sur le territoire français, la société Google France SARL. Cette société compte plusieurs centaines de salariés et s’est vue notifier l’ensemble des documents en lien avec la procédure. Elle relève également que les principales pièces à l’appui de la procédure (Règles de

confidentialité, Conditions d'utilisation, etc.) étaient les propres documents de la société, disponibles par ailleurs en anglais sur d'autres supports.

Au regard de ces éléments, la formation restreinte considère que la société disposait en tout état de cause de ressources matérielles et humaines suffisantes lui permettant d'assurer une traduction des documents en anglais dans un délai suffisant pour en prendre connaissance et formuler ses observations dans le délai qui lui était fixé.

La formation restreinte rappelle ensuite que l'article 75 du décret n° 2005-1309 du 20 octobre 2005 modifié prévoit que le responsable de traitement dispose d'un délai d'un mois pour formuler des observations en réponse au rapport qui lui a été adressé, puis d'un nouveau délai de quinze jours faisant suite au délai imparti au rapporteur pour apporter sa réponse.

La formation restreinte souligne qu'il a été fait droit aux demandes formulées par la société le 11 décembre 2018 visant à obtenir une extension de délai pour produire ses observations en réponse aux éléments apportés par le rapporteur et un report de séance. Ce report lui a permis de bénéficier d'un délai supplémentaire de quinze jours pour produire ses secondes observations par rapport au délai initialement prévu et préparer ainsi sa défense en vue de la séance de la formation restreinte. Elle a par ailleurs été en mesure de présenter ses observations orales le jour de la séance de la formation restreinte en complément de ses productions écrites.

La formation restreinte rappelle enfin que les constatations de fait opérées dans le cadre de la présente procédure portaient essentiellement sur des documents institutionnels rédigés par la société elle-même.

Au regard de ces éléments, la formation restreinte estime que les droits de la défense de la société Google LLC. ont été garantis.

3. Sur le périmètre des investigations

En défense, la société soutient tout d'abord que le rapporteur a confondu le système d'exploitation Android et le compte Google alors qu'il s'agit de services distincts qui mettent en œuvre des activités de traitements différentes.

Elle indique notamment que lors de la configuration de son appareil mobile sous Android, les utilisateurs ont clairement le choix de créer ou non un compte Google et que les Règles de confidentialité leur expliquent la manière dont les services Google peuvent être utilisés avec ou sans compte Google (ex : visionnage de vidéos YouTube sans création de compte etc.).

Elle fait ensuite valoir que le périmètre du contrôle choisi par la CNIL - à savoir la création d'un compte Google lors de la configuration d'un nouvel appareil utilisant le système d'exploitation Android - est limité en ce qu'il représente un cas de figure qui ne concerne que 7% des utilisateurs.

Enfin, elle indique que les constatations ont été effectuées sur une ancienne version du système d'exploitation Android.

Tout d'abord, la formation restreinte indique qu'elle ne remet pas en cause l'existence de services distincts, liés respectivement au système d'exploitation Android et au compte Google, mettant en œuvre des activités de traitements différentes.

Elle observe cependant que les faits couverts par les investigations correspondent au scénario retenu pour effectuer le contrôle en ligne, à savoir le parcours d'un utilisateur et les documents auxquels il pouvait avoir accès lors de la configuration initiale de son équipement mobile utilisant le système d'exploitation Android. Ce parcours incluait la création d'un compte. Ces faits se rapportent donc aux traitements couverts par la politique de confidentialité présentée à l'utilisateur lors de la création de son compte à l'occasion de la configuration de son téléphone mobile sous Android.

Ensuite, s'il est exact que l'utilisateur a effectivement le choix de créer un compte et a la possibilité d'utiliser certains des services de la société sans avoir à créer un compte, elle constate toutefois que lors de la configuration d'un appareil sous Android, la possibilité de créer un compte Google ou de se connecter à un compte déjà existant apparait naturellement au début du processus de paramétrage, sans action spécifique de l'utilisateur.

Celui-ci est par ailleurs invité à créer ou à se connecter à un compte Google dans la mesure où lorsqu'il clique sur les liens en savoir plus ou ignorer disponibles à cette étape de configuration de l'appareil, il se voit présenter l'information suivante : Votre appareil fonctionne mieux avec un compte Google, Si vous n'avez pas de compte Google, vous ne pourrez pas effectuer les actions suivantes […] Activer les fonctionnalités de protection de l'appareil.

La formation restreinte considère ainsi que ce parcours, lors de la création d'un compte, crée un continuum d'usage entre les traitements opérés par le système d'exploitation et ceux opérés au travers du compte Google, et justifie le scénario retenu pour le contrôle en ligne. Cette succession des informations et choix présentés à l'utilisateur ne fait toutefois pas obstacle à une analyse différenciée, au regard du

cadre juridique, des différentes activités de traitement en cause sur la base de l'ensemble des faits constatés dans le cadre de ce scénario de contrôle.

En outre, s'agissant des observations formulées par la société selon lesquelles ce cas de figure ne concernerait que 7% des utilisateurs – la plupart des utilisateurs d'un appareil fonctionnant sous Android se connectant à un compte préexistant - la formation restreinte rappelle qu'aux termes de l'article 11.I.2 de la loi informatique et libertés, la CNIL dispose d'un large pouvoir d'appréciation quant aux périmètres des contrôles qu'elle peut entreprendre. Un scénario spécifique de contrôle, tel que celui retenu en l'espèce, peut permettre d'opérer des constatations traduisant une politique de confidentialité plus globale.

Au demeurant, la formation restreinte relève que la société indique dans ses observations en date du 7 décembre 2018 que : la portée du traitement des données à caractère personnel qui est effectué pour les détenteurs d'un Compte Google lorsqu'ils utilisent un appareil sous Android est en grande partie similaire au traitement qui se produit pour les détenteurs d'un Compte Google lorsqu'ils utilisent les services Google sur un ordinateur ou sur un appareil ne fonctionnant pas sous Android et que [..] Présenter les mêmes Règles de confidentialité et Conditions d'Utilisation permet d'assurer une cohérence et une connaissance des utilisateurs et, de manière importante, fait office de rappel aux détenteurs de comptes existants de la nature de la collecte des données et des finalités de celle-ci. Dès lors, les utilisateurs qui configureraient leur mobile sous Android en y associant un compte déjà existant se trouvent, s'agissant de l'information qui leur est communiquée, dans une situation analogue aux utilisateurs qui procéderaient à la création d'un compte.

Enfin, s'agissant de la version du système d'exploitation Android utilisée pour procéder aux constatations, la formation restreinte relève que l'argument avancé par la société est sans incidence dès lors qu'il ressort des pièces fournies par la société que le parcours d'un utilisateur est similaire dans une version plus récente du système d'exploitation.

Au demeurant, la formation restreinte relève que les statistiques de répartition de l'utilisation des versions successives du système d'exploitation Android, mises à disposition sur le site officiel des développeurs Android (https://developer.android.com/about/dashboards/) démontrent que la version utilisée lors du contrôle fait partie des versions les plus utilisées (statistiques portant sur une période d'une semaine d'octobre 2018 à partir des données de connexions des terminaux s'étant connectés au Google Play Store).

4. Sur le manquement aux obligations de transparence et d'information

Le 1. de l’article 12 du Règlement général sur la protection des données dispose : 1. Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique. Lorsque la personne concernée en fait la demande, les informations peuvent être fournies oralement, à condition que l'identité de la personne concernée soit démontrée par d'autres moyens.

Le 1 de l’article 13 de ce même texte prévoit que : Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes les informations suivantes :

l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;

le cas échéant, les coordonnées du délégué à la protection des données ;

les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;

lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;

les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent ; et

le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition ; […] .

Le rapporteur estime que les informations délivrées aux utilisateurs par la société ne répondent pas aux objectifs d’accessibilité, de clarté et de compréhension fixés

par l'article 12 et que certaines informations rendues obligatoires par l'article 13 ne sont pas fournies aux utilisateurs.

En défense, la société considère que l'information qu'elle diffuse à ses utilisateurs répond aux exigences des articles 12 et 13 du RGPD.

Elle estime tout d'abord que le document intitulé Règles de confidentialité et conditions d'utilisation, accessible lors de la création d'un compte, constitue une information de premier niveau conforme aux lignes directrices du CEPD sur la transparence au sens du Règlement UE 2016/679 (WP260) du 25 mai 2018. Elle précise que ce document offre une bonne vue d'ensemble des traitements mis en œuvre et que la mention de la base juridique de ces traitements n'a pas à figurer dans ce premier niveau d'information. Les informations concernant la durée de conservation des données figurent quant à elles dans la rubrique Exporter et supprimer vos informations au sein des Règles de confidentialité.

La société fait ensuite valoir que l'information des personnes doit, au regard des articles 12 et 13 du Règlement, s'apprécier de façon globale. Elle expose à ce titre que l'information qu'elle délivre s'opère également, en complément des documents intitulés Règles de confidentialité et conditions d'utilisation, Règles de confidentialité et Conditions d'utilisation, par le biais de plusieurs autres modalités. Elle explique que des messages d'informations additionnelles peuvent apparaitre lors de la création d'un compte sous chacun des paramètres de confidentialité. Par ailleurs un message électronique est adressé à l'utilisateur au moment de la création de son compte indiquant notamment que : Vous pouvez à tout moment modifier les paramètres de confidentialité et de sécurité de votre compte Google, créer des rappels pour vous souvenir de vérifier vos paramètres de confidentialité ou procéder à une vérification de vos paramètres de sécurité. Ce message électronique contient des liens cliquables renvoyant à différents outils de paramétrage.

Ces autres outils de contrôle, qui sont mis à la disposition de l'utilisateur postérieurement à la création de son compte à partir de l'interface de gestion de son compte comportent par exemple un outil intitulé check-up confidentialité qui permet aux utilisateurs de choisir les réglages de confidentialité qui leur conviennent, y compris en matière d'annonces personnalisées, d'historique des positions, d'activité sur le Web et d'applications.

La société met aussi en avant un outil Dashboard qui permet aux utilisateurs d'avoir une vision d'ensemble de l'utilisation qu'ils font des services proposés par Google tels que Gmail ou Youtube.

Enfin, la société rappelle que lorsqu'un utilisateur a cliqué sur Créer un compte sans avoir désactivé les paramètres relatifs aux annonces personnalisées, une fenêtre pop-up de confirmation de création de compte s'affiche pour rappeler que le compte est configuré pour inclure des fonctionnalités de personnalisation. La société indique que le parcours utilisateur est ainsi configuré pour ralentir la progression des utilisateurs qui n'auraient pas fait spontanément le choix de paramètres plus protecteurs de la vie privée.

Au préalable, la formation restreinte prend acte des progrès réalisés ces dernières années par la société dans sa politique d'information des utilisateurs, dans le sens de la plus grande transparence et d'une maîtrise renforcée sur leurs données attendues par ceux-ci. Pour les raisons qui suivent toutefois, elle estime que les exigences du RGPD, dont la mise en œuvre doit être appréciée à l'aune de la portée concrète des traitements de données à caractère personnel en cause, ne sont pas respectées.

En premier lieu, la formation restreinte rappelle qu'en application des dispositions de l'article 12 du Règlement, les informations doivent être fournies de façon aisément accessible. Cette exigence d'accessibilité est éclairée par les lignes directrices sur la transparence, dans lesquelles le CEPD a considéré qu'un aspect primordial du principe de transparence mis en lumière dans ces dispositions est que la personne concernée devrait être en mesure de déterminer à l'avance ce que la portée et les conséquences du traitement englobent afin de ne pas être prise au dépourvu à un stade ultérieur quant à la façon dont ses données à caractère personnel ont été utilisées. […] Plus particulièrement, en ce qui concerne les traitements de données complexes, techniques ou non prévus, la position du G29 est que les responsables du traitement devraient […] définir séparément et de façon claire les principales conséquences du traitement : autrement dit, quel sera réellement l'effet du traitement spécifique décrit dans une déclaration ou un avis sur la protection de la vie privée pour la personne concernée . La formation restreinte rappelle en outre que l'obligation d'accessibilité posée par l'article 12 repose en partie sur les choix ergonomiques faits par le responsable du traitement.

En l'espèce, la formation restreinte constate que l'architecture générale de l'information choisie par la société ne permet pas de respecter les obligations du Règlement. En effet, les informations qui doivent être communiquées aux personnes en application de l'article 13 sont excessivement éparpillées dans plusieurs documents : Règles de confidentialité et conditions d'utilisation , affiché au cours de la création du compte, puis Conditions d'utilisation et Règles de confidentialité qui sont accessibles dans un deuxième temps au moyen de liens cliquables figurant sur le premier document. Ces différents documents comportent

des boutons et liens qu'il est nécessaire d'activer pour prendre connaissance d'informations complémentaires. Un tel choix ergonomique entraine une fragmentation des informations obligeant ainsi l'utilisateur à multiplier les clics nécessaires pour accéder aux différents documents. Celui-ci doit ensuite consulter attentivement une grande quantité d'informations avant de pouvoir identifier le ou les paragraphes pertinents. Le travail fourni par l'utilisateur ne s'arrête toutefois pas là puisqu'il devra encore recouper et comparer les informations collectées afin de comprendre quelles données sont collectées en fonction des différents paramétrages qu'il aura pu choisir.

La formation restreinte relève que, compte tenu de cette architecture, certaines informations sont difficilement trouvables.

Par exemple, s'agissant des traitements de personnalisation de la publicité, pour connaitre les informations qui sont collectées auprès de lui pour cette finalité, un utilisateur doit accomplir de nombreuses actions et combiner plusieurs ressources documentaires. Dans un premier temps, il doit prendre connaissance du document général Règles de confidentialité et conditions d'utilisation, puis cliquer sur le bouton Plus d'options et ensuite sur le lien En savoir plus pour que soit affichée la page Personnalisation des annonces. Il aura ainsi accès à une première description du traitement relatif à la personnalisation de la publicité qui s'avère être incomplète. Pour compléter l'information relative aux données traitées dans le cadre de cette finalité, l'utilisateur devra encore consulter dans son intégralité la rubrique proposer des services personnalisés contenue dans le document Règles de confidentialité, lui-même accessible depuis le document général Règles de confidentialité et conditions d'utilisation.

De même, en matière de traitement des données de géolocalisation, la formation restreinte relève qu'un même parcours dénué de tout caractère intuitif est requis de l'utilisateur s'agissant des informations relatives aux données de géolocalisation. Celui-ci devra en effet accomplir les étapes suivantes : Consulter les Règles de confidentialité et conditions d'utilisation , cliquer sur Plus d'options puis sur le lien En savoir plus pour que soit affichée la page Historique des positions et prendre connaissance du texte affiché. Ce texte ne constituant toutefois qu'une courte description du traitement, l'utilisateur devra, pour accéder au reste des informations, retourner au document Règles de confidentialité et consulter la rubrique Informations relatives à votre position géographique . L'information ne sera toujours pas complète puisque cette rubrique contient plusieurs liens cliquables relatifs aux différentes sources utilisées pour le géolocaliser.

Dans les deux cas de figures décrits, cinq actions sont nécessaires à l'utilisateur pour accéder à l'information relative à la personnalisation des annonces et six en ce qui concerne la géolocalisation.

La formation restreinte relève encore que si l'utilisateur souhaite disposer d'information sur les durées de conservation de ses données personnelles, il doit tout d'abord consulter les Règles de confidentialité qui se trouvent dans le document principal, puis se rendre dans la rubrique intitulée Exporter et supprimer vos informations et enfin cliquer sur le lien hypertexte cliquer ici contenu dans un paragraphe général sur les durées de conservations. Ce n'est donc qu'au bout de quatre clics que l'utilisateur accède à cette information. La formation restreinte constate au demeurant que le titre choisi par la société pour Exporter et supprimer vos informations ne permet pas facilement à l'utilisateur de comprendre qu'il s'agit d'une rubrique permettant d'accéder aux informations relatives aux durées de conservation. **Dès lors, la formation restreinte estime dans ce cas de figure que la multiplication des actions nécessaires, combinée à un choix de titres non explicites ne satisfait pas aux exigences de transparence et d'accessibilité de l'information.**

Il résulte de l'ensemble de ces éléments un défaut global d'accessibilité des informations délivrées par la société dans le cadre des traitements en cause.

En deuxième lieu, la formation restreinte considère que le caractère clair et compréhensible des informations délivrées, exigé par l'article 12 du RGPD, doit s'apprécier en tenant compte de la nature de chaque traitement en cause et de son impact concret sur les personnes concernées.

Au préalable, il est essentiel de souligner que les traitements de données mis en œuvre par le responsable de traitement sont particulièrement massifs et intrusifs.

Les données collectées par Google proviennent de sources extrêmement variées. Ces données sont collectées à la fois à partir de l'utilisation du téléphone, de l'utilisation des services de la société, tels que le service de messagerie Gmail ou la plateforme de vidéos Youtube, mais aussi à partir des données générées par l'activité des utilisateurs lorsqu'ils se rendent sur des sites tiers utilisant les services Google grâce notamment aux cookies Google analytics déposés sur ces sites.

A ce titre, les Règles de confidentialité laissent apparaître qu'au moins vingt services proposés par la société sont susceptibles d'être impliqués dans les traitements, pouvant concerner des données telles que l'historique de navigation web, l'historique d'usage des applications, les données stockées localement sur l'équipement (telles que les carnets d'adresses), la géolocalisation de l'équipement,

etc. Dès lors, un grand nombre de données est traité dans le cadre de ces services via ou en lien avec le système d'exploitation Android.

Il ressort de l'instruction du dossier qu'outre les données de sources externes, la société traite au moins trois catégories de données :

des données produites par la personne (par exemple, son nom, son mot de passe, son numéro de téléphone, son adresse courriel, un moyen de paiement, des contenus créés, importés ou reçus, tels que des écrits, des photos ou des vidéos) ;

des données générées par son activité (par exemple, l'adresse IP, des identifiants uniques de l'utilisateur, les données de réseau mobile, les données liées aux réseaux sans fil et aux appareils Bluetooth, l'horodatage des actions effectuées, les données de géolocalisation, les données techniques des appareils utilisés y compris les données relatives aux capteurs (accéléromètre, etc.), les vidéos vues, les recherches effectuées, l'historique de navigation, les achats, les applications utilisées, etc. ;

des données dérivées ou inférées à partir des données fournies par cette personne ou son activité. S'agissant de cette catégorie, les Règles de confidentialité listent un certain nombre de finalités qui ne peuvent être accomplies qu'en générant des données à partir des deux autres catégories de données. Ainsi, la personnalisation des annonces que la société réalise nécessite d'inférer les centres d'intérêt des utilisateurs à partir de leur activité afin de pouvoir proposer ceux-ci aux annonceurs. De la même manière, les finalités de fourniture de contenus, de recherches et de recommandations personnalisés nécessitent d'inférer de nouvelles informations à partir de celles déclarées, produites ou générées par l'activité de la personne.

Par ailleurs, si le très grand nombre de données traitées permet de caractériser à lui seul le caractère massif et intrusif des traitements opérés, la nature même de certaines des données décrites, telles que les données de géolocalisation ou les contenus consultés, renforce ce constat. Considérée isolément, la collecte de chacune de ces données est susceptible de révéler avec un degré de précision important de nombreux aspects parmi les plus intimes de la vie des personnes, dont leurs habitudes de vie, leurs goûts, leurs contacts, leurs opinions ou encore leurs déplacements. Le résultat de la combinaison entre elles de ces données renforce considérablement le caractère massif et intrusif des traitements dont il est question.

En conséquence, c'est à la lumière des caractéristiques particulières de ces traitements de données à caractère personnel qui viennent d'être rappelées que les caractères clair et compréhensible, au sens de l'article 12 du RGPD, des informations

prévues à l'article 13 du Règlement, doivent être appréciés. La formation restreinte considère que ces exigences ne sont, en l'espèce, pas respectées.

Concrètement, la formation restreinte relève que les informations délivrées par la société ne permettent pas aux utilisateurs de comprendre suffisamment les conséquences particulières des traitements à leur égard.

En effet, les finalités annoncées dans les différents documents sont ainsi décrites : proposer des services personnalisés en matière de contenu et d'annonces, assurer la sécurité des produits et services, fournir et développer des services, etc. Elles sont trop génériques au regard de la portée des traitements mis en œuvre et de leurs conséquences. C'est également le cas lorsqu'il est indiqué aux utilisateurs de manière trop vague : Les informations que nous collectons servent à améliorer les services proposés à tous nos utilisateurs. […] Les informations que nous collectons et l'usage que nous en faisons dépendent de la manière dont vous utilisez nos services et dont vous gérez vos paramètres de confidentialité.

La formation restreinte relève, par suite, que la description des finalités poursuivies ne permet pas aux utilisateurs de mesurer l'ampleur des traitements et le degré d'intrusion dans leur vie privée qu'ils sont susceptibles d'emporter. Elle estime, en particulier, qu'une telle information n'est pas apportée de manière claire, ni au premier niveau d'information fourni aux utilisateurs par le biais, en l'espèce, du document intitulé Règles de confidentialité et conditions d'utilisation, ni dans les autres niveaux d'information proposés par la société.

La formation restreinte constate en outre que la description des données collectées, qui pourrait être de nature à éclairer la portée de ces finalités et à éviter que l'utilisateur soit pris ultérieurement au dépourvu quant à la façon dont ses données ont été utilisées et combinées, est particulièrement imprécise et incomplète, tant à l'analyse du premier niveau d'information que de celle des autres documents fournis.

Ainsi, le document Règles de confidentialité et conditions d'utilisation ainsi que le document intitulé Règles de confidentialité précisent : Il peut s'agir d'informations (…) plus complexes, comme les annonces que vous trouvez les plus utiles, les personnes qui vous intéressent le plus sur le Web ou les vidéos YouTube qui sont susceptibles de vous plaire.

Au regard de ce qui précède, la formation restreinte estime que l'utilisateur n'est pas en mesure, en particulier en prenant connaissance du premier niveau d'information qui lui est présenté dans les Règles de confidentialité et conditions

d'utilisation, de mesurer la portée des principaux traitements sur sa vie privée. Si elle prend acte de ce qu'une information exhaustive, dès le premier niveau, serait contreproductive et ne respecterait pas l'exigence de transparence, elle estime que celui-ci devrait contenir des termes de nature à objectiver le nombre et la portée des traitements mis en œuvre. Elle considère en outre qu'il serait possible, par d'autres types de modalités de présentation adaptées à des services de combinaison de données, de fournir dès le stade des Règles de confidentialité une vision d'ensemble des caractéristiques de cette combinaison en fonction des finalités poursuivies.

Le constat du défaut de clarté et de caractère compréhensible doit être également fait s'agissant de la mention de la base juridique des traitements de personnalisation de la publicité. En effet, la société indique tout d'abord dans les Règles de Confidentialité : Nous vous demandons l'autorisation de traiter vos informations à des fins spécifiques, et vous êtes libre de revenir sur votre consentement à tout moment. Par exemple, nous vous demandons l'autorisation de vous fournir des services personnalisés, tels que des annonces […]. La base juridique retenue ici apparait donc être le consentement. Toutefois, la société ajoute plus loin se fonder sur l'intérêt légitime, notamment pour mener des actions de marketing en vue de faire connaître nos services auprès des utilisateurs et surtout avoir recours à la publicité afin de rendre un grand nombre de nos services disponibles gratuitement pour les utilisateurs.

La formation restreinte souligne que si devant elle, la société a indiqué que la seule base juridique sur laquelle repose le traitement relatif à la publicité personnalisée est le consentement, il ressort de l'instruction que cette clarification n'est pas portée à la connaissance des utilisateurs. Les formulations rappelées ci-dessus ne permettent pas à ces derniers de mesurer clairement la distinction entre la publicité proprement personnalisée, à partir de la combinaison de multiples données relatives à l'utilisateur, qui repose d'après les dires de la société sur le consentement, d'autres formes de ciblage utilisant par exemple le contexte de navigation, fondées sur l'intérêt légitime. La formation restreinte souligne l'importance particulière de l'exigence de clarté s'agissant de ces traitements, compte tenu de leur place dans les traitements mis en œuvre par la société et de leur impact sur les personnes dans l'économie numérique.

S'agissant de l'information relative aux durées de conservation, la formation restreinte relève que la page Comment les informations collectées par Google sont-elles conservées comporte quatre catégories :

Informations conservées jusqu'à ce que vous les supprimiez ;

Informations assorties d'un délai d'expiration ;

Informations conservées jusqu'à la suppression de votre compte Google ;

Informations conservées pendant de longues périodes pour des raisons précises.

Elle constate néanmoins que s'agissant de la dernière catégorie, seules des explications très générales sur la finalité de cette conservation sont fournies et aucune durée précise ni les critères utilisés pour déterminer cette durée ne sont indiqués. Or cette information figure parmi celles devant être obligatoirement délivrées aux personnes en application du a) du °2 de l'article 13 du Règlement.

En dernier lieu, si la société fait valoir que de multiples outils d'information sont mis à la disposition des utilisateurs concomitamment et après la création de leur compte, la formation restreinte relève que ces modalités ne permettent pas d'atteindre les exigences de transparence et d'information issues des articles 12 et 13 du RGPD.

Tout d'abord, la formation restreinte relève que les outils auxquels la société fait référence contribuent effectivement, dans une certaine mesure, à l'objectif de transparence tout au long de la vie du compte et de l'utilisation des services de Google. Cependant, la formation restreinte considère qu'ils ne participent pas de manière suffisante à l'information prévue par l'article 13, qui doit intervenir au moment où les données en question sont obtenues. Ainsi que l'ont rappelé les lignes directrices du CEPD sur la transparence, l'article 13 indique les informations à fournir aux personnes concernées dès la phase de commencement du cycle de traitement.

Si des données autres que celles strictement nécessaires à la création du compte, sont collectées tout au long de la vie du compte, telles que l'historique de navigation ou des achats, le moment de sa création marque l'entrée de l'utilisateur dans l'écosystème des services Google, dont le caractère particulièrement massif et intrusif des traitements a été rappelé précédemment. Cette étape marque le début d'une multitude d'opérations de traitements : collecte, combinaison, analyse etc. Par conséquent, dans la mesure où le processus de création du compte est primordial dans l'appréhension des traitements et de leur impact et où le parcours utilisateur proposé invite lui-même la personne concernée à concentrer tout particulièrement son attention à ce stade, l'information prévue à l'article 13 du Règlement qui intervient à ce moment doit, par elle-même, être suffisante au regard des exigences résultant de cette disposition ainsi que de l'article 12 du même règlement.

Au demeurant, tant la fenêtre pop-up surgissant au moment de la création du compte que le message électronique envoyé dès la création du compte ne contiennent que des informations sommaires ou très ciblées sur les traitements mis en œuvre et ne sauraient permettre de regarder l'information préalable comme suffisante.

Le texte de la fenêtre pop-up indique en effet Ce compte Google est configuré pour inclure des fonctionnalités de personnalisation (telles que les recommandations et les annonces personnalisées) qui sont basées sur les informations enregistrées dans votre compte. Le message électronique indique quant à lui les principales fonctionnalités du compte Google et l'existence d'outils de contrôle.

S'agissant de l'outil check-up confidentialité celui-ci permet essentiellement à l'utilisateur de paramétrer les informations collectées tels que l'historique de navigation ou des lieux fréquentés. Enfin, le Dashboard consiste en un panneau d'information regroupant pour chaque service Google un aperçu des habitudes d'utilisation du titulaire du compte.

Néanmoins, ces outils check-up confidentialité et Dashboard ne sont mobilisables, tout comme d'ailleurs le message électronique mentionné ci-dessus, que postérieurement à l'étape de création du compte, laquelle est pourtant primordiale pour l'information des utilisateurs ainsi qu'il a été dit**. En outre, bien que leur existence et leur intérêt soient portés à la connaissance des utilisateurs, ils supposent une démarche active et d'initiative de ceux-ci. Pour ces raisons, ces outils ne permettent pas de considérer qu'une information suffisante est délivrée pour l'application de l'article 13 du Règlement.**

Au regard de l'ensemble de ces éléments, la formation restreinte considère qu'un manquement aux obligations de transparence et d'information telles que prévues par les articles 12 et 13 du Règlement est caractérisé.

5. Sur le manquement à l'obligation de disposer d'une base légale pour les traitements mis en œuvre

L'article 6 du RGPD dispose que : Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;

le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;

le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Il était reproché à la société de ne pas recueillir valablement le consentement des personnes pour les traitements de personnalisation de la publicité. Il était également considéré que la société ne pouvait se prévaloir d'un intérêt légitime pour ces mêmes traitements.

En défense, la société précise qu'elle se fonde uniquement sur le consentement pour les traitements de personnalisation de la publicité.

L'article 4 (11) du Règlement susvisé précise ce que l'on entend par consentement : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

L'article 7 de ce même texte prévoit les conditions qui lui sont applicables :

1. Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.

2. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en

des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.

3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.

4. Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée.

En premier lieu, la société affirme que le consentement des utilisateurs est éclairé.

Elle estime que des informations simples et claires sont présentées à l'utilisateur lors de la création d'un compte et lui permettent d'avoir connaissance de la manière dont la société utilise les données à des fins de personnalisation de la publicité. La société fait notamment référence au résumé intitulé Règles de confidentialité et conditions d'utilisation, aux sections dédiées à la personnalisation des annonces contenues dans les Règles de confidentialité ainsi qu'au message d'information additionnelle intitulé Personnalisation de la publicité apparaissant dans les options de paramétrage de création du compte.

En second lieu, la société affirme que le consentement des utilisateurs est spécifique et univoque.

Elle fait notamment valoir que lors du paramétrage du compte, l'utilisateur a la possibilité de faire un choix quant à l'affichage de la personnalisation de la publicité. Elle estime que cette possibilité lui permet d'exprimer son consentement sur l'utilisation de ses données indépendamment des autres choix qu'il peut exprimer s'agissant des autres finalités relatives aux traitements associés au compte Google (ex. historique des recherches YouTube).

Elle considère par ailleurs que les modalités de recueil du consentement à des fins de personnalisation des annonces qu'elle met en place sont conformes aux recommandations de la CNIL du 5 décembre 2013 en matière de cookies. Elle précise notamment que sont disponibles des informations succinctes sur la personnalisation des annonces suivies par un bouton "j'accepte" (les Règles de confidentialité et les Conditions d'utilisation), précédé par un bouton "plus d'options" qui donne aux utilisateurs la possibilité de désactiver plusieurs opérations de traitement, y compris à des fins de personnalisation des annonces.

Elle soutient également que la solution admise dans la mise en demeure publique de la présidente de la CNIL n° MED-2018-023 du 29 novembre 2018 permet à l'utilisateur de consentir à l'ensemble des finalités via un bouton tout accepter.

Enfin, elle estime qu'un consentement explicite pour le traitement de données à des fins de personnalisation de la publicité, au sens du a) du 2 de l'article 9 du RGPD, ne pourrait être exigé dès lors qu'il ne s'agit pas de données sensibles.

En ce qui concerne le caractère éclairé

Au préalable, la formation restreinte précise que ce caractère éclairé doit être examiné à la lumière des développements précédents concernant le défaut de transparence et d'information des utilisateurs lors de la création de leur compte. Elle considère en effet que les manquements précédemment identifiés ont nécessairement une incidence sur l'information délivrée aux utilisateurs pour assurer le caractère éclairé du consentement.

La formation restreinte indique que les lignes directrices du CEPD du 10 avril 2018 sur le consentement au sens du Règlement 2016/679 (WP250) précisent : le responsable du traitement doit s'assurer que le consentement est fourni sur la base d'informations qui permettent aux personnes concernées d'identifier facilement qui est le responsable des données et de comprendre ce à quoi elles consentent. [Il] doit clairement décrire la finalité du traitement des données pour lequel le consentement est sollicité.

Ces lignes directrices précisent également que : Pour que le consentement soit éclairé, il est nécessaire d'informer la personne concernée de certains éléments cruciaux pour opérer un choix. [..] Au moins les informations suivantes sont nécessaires afin d'obtenir un consentement valable :

l'identité du responsable du traitement,

la finalité de chacune des opérations de traitement pour lesquelles le consentement est sollicité,

les (types de) données collectées et utilisées,

l'existence du droit de retirer son consentement,

des informations concernant l'utilisation des données pour la prise de décision automatisée [..] et

des informations sur les risques éventuels liés à la transmission des données en raison de l'absence de décision d'adéquation et de garanties appropriées […].

Comme elle a pu le relever au titre du manquement aux obligations de transparence et d'information, la formation restreinte considère que l'information sur les traitements de personnalisation de la publicité est excessivement disséminée dans des documents distincts et qu'elle n'est, à ce titre, pas aisément accessible. A cet égard, la formation restreinte renvoie aux développements précédents sur les multiples actions qui doivent être faites par un utilisateur qui souhaite prendre connaissance des informations disponibles sur les traitements liés à la personnalisation de la publicité.

En outre, comme cela a également été relevé au titre du manquement aux obligations de transparence, l'information fournie n'est pas suffisamment claire et compréhensible en ce qu'il est difficile pour un utilisateur d'avoir une appréhension globale des traitements dont il peut faire l'objet et de leur portée.

A titre d'illustration, l'information diffusée dans la rubrique Personnalisation des annonces, accessible depuis le document Règles de confidentialité et conditions d'utilisation via le bouton Plus d'options, contient la mention suivante : Google peut vous présenter des annonces en fonction de votre activité au sein de services Google (dans la recherche ou sur YouTube par exemple, ainsi que sur les sites Web et les applications partenaires de Google) . La formation restreinte relève qu'il n'est pas possible de prendre connaissance, par exemple par le biais de liens cliquables, des services, sites et application de Google auxquels la société fait référence. Dès lors, l'utilisateur n'est pas en mesure de comprendre les traitements de personnalisation de la publicité dont ils font l'objet, ainsi que leur portée, alors même que ces traitements impliquent pourtant une pluralité de services (par exemple : Google search, YouTube, Google home, Google maps, Playstore, Google photo, Google play, Google analytics, Google traduction, Play livres) et le traitement de très nombreuses données à caractère personnel. Les utilisateurs ne sont pas en mesure d'avoir une juste perception de la nature et du volume des données qui sont collectées.

Au vu de ces éléments, la formation restreinte considère que le consentement des utilisateurs pour les traitements de personnalisation de la publicité n'est pas suffisamment éclairé.

S'agissant du caractère spécifique et univoque du consentement

Le considérant 32 du Règlement prévoit que : Le consentement doit être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant […]. Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité.

Le considérant 43 du RGPD précise que : Le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce.

Les lignes directrices du CEPD sur le consentement susvisées précisent que : Afin de se conformer au caractère spécifique du consentement, le responsable du traitement doit garantir : […] (ii) le caractère détaillé des demandes de consentement […] Cela signifie qu'un responsable du traitement qui sollicite le consentement pour diverses finalités spécifiques devrait prévoir un consentement distinct pour chaque finalité afin que les utilisateurs puissent donner un consentement spécifique à des finalités spécifiques .

En l'espèce, la formation restreinte relève que lorsque l'utilisateur crée un compte, il a la possibilité de modifier certains des paramètres associés au compte. Pour accéder à ces paramètres, l'utilisateur doit cliquer sur le bouton plus d'options, présent avant le bouton Créer un compte. La formation restreinte relève par ailleurs que les paramètres de personnalisation du compte, qui contiennent le choix en matière d'affichage des annonces personnalisées, sont pré-cochés par défaut, ce qui traduit, sauf action contraire, l'accord de l'utilisateur au traitement de ses données pour les finalités mentionnées (ex. historique des recherches YouTube, affichage des annonces personnalisées etc.). L'utilisateur a la possibilité de décocher ces paramètres s'il ne souhaite pas que ces traitements soient mis en œuvre.

La formation restreinte observe que, au moment de la création du compte, si l'utilisateur ne clique pas sur le bouton plus d'options afin de paramétrer son compte, il doit cocher les cases j'accepte les conditions d'utilisation de Google et j'accepte que mes informations soient utilisées telles que décrit ci-dessus et détaillées dans les règles de confidentialité. Par la suite, il doit appuyer sur le bouton Créer un compte. Une fenêtre surgissante apparaît, intitulée Simple confirmation qui contient le texte suivant Ce compte Google est configuré pour inclure des fonctionnalités de personnalisation (telles que les recommandations et les annonces personnalisées), qui sont basées sur les informations enregistrées dans votre compte. Pour modifier vos paramètres de personnalisation et les informations enregistrées dans votre compte, sélectionnez Plus d'options.

S'il ne clique pas sur Plus d'options, l'utilisateur doit alors sélectionner le bouton Confirmer pour finaliser la création du compte.

Au vu de ce qui précède, la formation restreinte relève que si l'utilisateur a la possibilité de modifier la configuration des paramètres de son compte préalablement

à sa création, une action positive de sa part est nécessaire pour accéder aux possibilités de paramétrage du compte. Ainsi, l'utilisateur peut tout à fait créer son compte, et accepter les traitements qui y sont liés, notamment les traitements de personnalisation de la publicité, sans cliquer sur Plus d'options. Par conséquent, le consentement de l'utilisateur n'est, dans ce cas de figure, pas valablement recueilli dans la mesure où il n'est pas donné par le biais d'un acte positif par lequel la personne consent spécifiquement et distinctement au traitement de ses données à des fins de personnalisation de la publicité par rapport aux autres finalités de traitement.

La formation restreinte considère en outre que les actions par lesquelles l'utilisateur procède à la création de son compte - en cochant les cases j'accepte les conditions d'utilisation de Google et j'accepte que mes informations soient utilisées telles que décrit ci-dessus et détaillées dans les règles de confidentialité, puis en sélectionnant Créer un compte - ne sauraient être considérées comme l'expression d'un consentement valable. Le caractère spécifique du consentement n'est pas respecté puisque l'utilisateur, par ces actions, accepte en bloc l'ensemble des traitements de données à caractère personnel mis en œuvre par la société, y compris à ceux de personnalisation de la publicité.

Par ailleurs, la formation restreinte relève que lorsqu'il clique sur Plus d'options pour accéder à la configuration des paramètres de son compte, ceux-ci, et notamment celui relatif à l'affichage des annonces personnalisées, sont tous pré-cochés par défaut. Aussi, la possibilité laissée aux utilisateurs de paramétrer leur compte ne se traduit pas non plus, dans ce cas de figure, par un acte positif ayant pour objet de recueillir le consentement, mais par une action ayant pour objet de permettre l'opposition au traitement.

La formation restreinte relève enfin que cette analyse est corroborée par les lignes directrices du G29 sur le consentement qui précisent que : Un responsable du traitement doit également être conscient que le consentement ne peut être obtenu moyennant la même action que lorsqu'une personne concernée accepte un contrat ou les conditions générales d'un service. [..]Le RGPD n'autorise pas les responsables du traitement à proposer des cases cochées par défaut ou des options de refus nécessitant une action de la personne concernée pour signaler son refus (par exemple des cases de refus).

La formation restreinte observe à ce titre que, si certains parcours utilisateurs peuvent inclure une fonctionnalité permettant à l'utilisateur de consentir de manière mutualisée au traitement de ses données pour différentes finalités proches, cette

facilité ne peut être considérée comme conforme que si les différentes finalités de traitement lui ont été présentées de manière distincte au préalable et qu'il a été en mesure de donner un consentement spécifique pour chaque finalité, par un acte positif clair, les cases n'étant pas pré-cochées. Pour que ce type de parcours utilisateurs puisse être considéré comme conforme, la possibilité de donner un consentement spécifique pour chaque finalité doit être offerte aux personnes avant la possibilité de tout accepter, ou de tout refuser, et ce sans qu'elles aient à faire d'action particulière pour y accéder, comme cliquer sur plus d'options. Au vu de ce qui précède, la formation retreinte considère que ce type de parcours utilisateurs offre des garanties différentes de celles proposées en l'espèce, ce parcours permettant à l'utilisateur de consentir spécifiquement et distinctement au traitement de ses données pour une finalité déterminée, par un acte positif clair, et cette possibilité lui étant offerte immédiatement et préalablement à la fonctionnalité tout accepter.

Dès lors, en l'espèce, en étant autorisés et masqués par défaut, les traitements de personnalisation de la publicité ne sauraient être considérés comme ayant été acceptés par l'utilisateur par un acte positif spécifique et univoque.

En deuxième lieu, si la société soutient que les modalités de recueil du consentement à des fins de personnalisation des annonces qu'elle met en place sont conformes aux recommandations de la CNIL du 5 décembre 2013 en matière de cookies, la formation restreinte rappelle que les règles spécifiquement applicables en matière de cookies liés aux opérations relatives à la publicité ciblée sont fixées par les dispositions distinctes de l'article 32-II de la loi informatique et libertés, résultant de la transposition de la directive ePrivacy du 12 juillet 2002 (modifiée par la directive 2009/136/CE). L'invocation de la recommandation du 5 décembre 2013 est par suite, et en tout état de cause, inopérante.

En troisième lieu, contrairement à ce que soutient Google, les exigences posées en matière de recueil du consentement ne visent pas à instaurer un régime de consentement qui serait plus protecteur que celui imposé par le RGPD et qui serait, à tort, défini au regard des critères imposés pour le recueil du consentement applicable en matière de traitement des données personnelles dites sensibles.

La formation restreinte relève que les modalités d'expression du consentement ont été précisées et définies par l'article 4 (11) du Règlement, qui indique que l'on entend par consentement : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par

un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Ces mêmes modalités d'expression du consentement s'appliquent de la même manière, que le consentement soit recueilli, au titre de l'article 6 du RGPD, pour la mise en œuvre d'un traitement pour une finalité spécifique, ou qu'il soit recueilli, en application de l'article 9 du RGPD, pour lever l'interdiction de principe posée au traitement de données à caractère personnel dites sensibles.

Par conséquent, pour pouvoir être considéré comme valable, le consentement recueilli doit être une manifestation volonté spécifique, éclairée et univoque ce qui, comme la formation restreinte l'a relevé précédemment, n'est pas le cas en l'espèce.

Au vu de l'ensemble de ces éléments, la formation restreinte considère que le consentement sur lequel se fonde la société pour les traitements de personnalisation de la publicité n'est pas valablement recueilli.

III. Sur la sanction et la publicité

L'article 45-III 7° de la loi du 6 janvier 1978 dispose : Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes:[…] : 7° À l'exception des cas où le traitement est mis en œuvre par l'État, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83.

La société considère qu'une amende administrative d'un montant de 50 millions d'euros est disproportionnée.

Elle relève qu'une mise en demeure lui aurait permis d'entreprendre une démarche de mise en conformité et qu'il n'apparait pas que le prononcé direct d'une amende administrative constitue la mesure correctrice la plus adéquate.

Elle considère en outre que les critères fixés à l'article 83 du RGPD n'ont pas tous été pris en compte dans l'évaluation de l'amende proposée. Sur ce point, elle fait notamment référence à l'impossibilité de prendre des mesures correctrices en raison de l'absence de mise en demeure préalable.

La société fait ensuite valoir le faible nombre d'utilisateurs concernés par les manquements et indique que sur […] personnes qui configurent un appareil sous le système d'exploitation Android par jour, seul […] personnes créent un compte.

Tout d'abord, la formation restreinte relève qu'en vertu de l'article 45 susvisé issu de la loi n° 2018-493 du 20 juin 2018, le Président de la CNIL dispose de l'opportunité des poursuites et peut donc choisir, en fonction des circonstances de l'espèce, les suites à apporter à des investigations en clôturant un dossier, en prononçant une mise en demeure ou en saisissant la formation restreinte en vue du prononcé d'une ou plusieurs mesures correctrices, sans qu'il appartienne au demeurant à cette dernière de se prononcer sur l'orientation choisie par le Président. La formation restreinte, ainsi saisie, est alors pleinement compétente pour se prononcer sur la matérialité et la qualification des faits, puis pour apprécier si les manquements qu'elle aurait caractérisés justifient, dans son principe même, le prononcé de l'une des mesures correctrices mentionnées au III de l'article 45 de la loi du 6 janvier 1978 et, enfin, pour se prononcer sur le montant d'une éventuelle amende.

En outre, la formation restreinte rappelle que si une administration, dans le cas où une décision est prise au regard d'un ensemble de critères prévus par un texte, doit tenir compte de l'ensemble de ces critères, elle n'est pas tenue dans la motivation de sa décision de se prononcer sur chacun d'entre eux mais peut se limiter à mentionner ceux qu'elle estime pertinents et les éléments de fait correspondants.

Dans le cas d'espèce, la formation restreinte estime que les faits et manquements précités justifient que soit prononcée une amende administrative à l'encontre de la société pour les motifs suivants.

En premier lieu, la formation restreinte tient à souligner la nature particulière des manquements relevés à la licéité du traitement et aux obligations de transparence et d'information. En effet, l'article 6 du RGPD - qui définit limitativement les cas de licéité d'un traitement - est une disposition centrale de la protection des données personnelles en ce qu'elle ne permet la mise en œuvre d'un

traitement que si l'une des six conditions listées est remplie. Les obligations de transparence et d'information sont également essentielles en ce qu'elles conditionnent l'exercice des droits des personnes et leur permettent donc de garder le contrôle sur leurs données. A cet égard, tant l'article 6 que les articles 12 et 13 figurent parmi les dispositions dont la méconnaissance est la plus sévèrement sanctionnée au 5. de l'article 83 du RGPD.

La formation restreinte considère ainsi que les obligations prévues en termes de transparence et de bases juridiques constituent des garanties fondamentales permettant aux personnes de garder la maîtrise de leurs données. La méconnaissance de ces obligations essentielles apparaît dès lors particulièrement grave, du fait de leur seule nature.

En deuxième lieu, la formation restreinte note que les manquements retenus perdurent à ce jour et sont des violations continues du Règlement. Il ne s'agit ni d'une méconnaissance ponctuelle de la société à ses obligations, ni d'une violation habituelle à laquelle le responsable du traitement aurait mis fin spontanément depuis la saisine de la formation restreinte.

En troisième lieu, la gravité des violations est à apprécier au regard notamment de la finalité des traitements, de leur portée et du nombre de personnes concernées.

A cet égard, la formation restreinte relève que si, selon la société, le scénario retenu pour les investigations en ligne menées par la CNIL correspond directement à seulement 7% de ses utilisateurs, le nombre de personnes ainsi concernées est, par lui-même, particulièrement important. Elle rappelle en outre que les utilisateurs qui configureraient leur mobile sous Android en y associant un compte déjà existant se trouvent, s'agissant des documents qui leurs sont communiqués et donc des violations retenues au Règlement, dans une situation analogue à ceux créant pour la première fois un compte, ce que la société n'a pas contesté dans son courrier du 7 décembre 2018.

En outre, la formation restreinte rappelle que la société met en place des traitements de données d'une ampleur considérable compte tenu de la place prépondérante qu'occupe le système d'exploitation Android sur le marché français des systèmes d'exploitation mobiles et de la proportion de recours aux ordiphones par les utilisateurs de téléphones en France. Ainsi, les données de millions d'utilisateurs sont traitées par la société dans ce cadre.

Les traitements couverts par la politique de confidentialité présentée à l'utilisateur lors de la création de son compte - à l'occasion de la configuration de son téléphone mobile sous Android - apparaissent également d'une envergure considérable au regard du nombre de services impliqués - a minima une vingtaine - et de la variété des données traitées via ou en lien avec le système d'exploitation Android. Outre les données fournies par l'utilisateur lui-même lors de la création du compte et de l'utilisation du système d'exploitation, la formation restreinte rappelle qu'une multitude de données issues de son activité est également générée telle que l'historique de navigation web, l'historique d'usage des applications, la géolocalisation de l'équipement, les achats etc. De même, des données sont déduites d'informations fournies par la personne concernée ou son activité, notamment dans le cadre de la personnalisation des annonces. Il s'agit donc d'informations nombreuses et particulièrement éclairantes sur les habitudes de vie des personnes, leurs opinions et interactions sociales. Partant, les données traitées par la société touchent au plus près leur identité et leur intimité.

De plus, la formation restreinte note que des multiples procédés technologiques sont utilisés par la société afin de combiner et analyser des données provenant de différents services, applications ou sources externes. Ils ont indéniablement un effet multiplicateur quant à la connaissance précise que la société a de ses utilisateurs.

En conséquence, la formation restreinte estime que la société dispose d'opérations de combinaisons au potentiel quasi illimité permettant un traitement massif et intrusif des données des utilisateurs.

Compte tenu de la portée des traitements de données - notamment celui de personnalisation de la publicité - et du nombre de personnes concernées, la formation restreinte souligne que les manquements précédemment retenus revêtent une particulière gravité. Un défaut de transparence concernant ces traitements d'ampleur, tout comme l'une absence de consentement valide des utilisateurs au traitement de personnalisation de la publicité constituent des atteintes substantielles à la protection de leur vie privée et se situent à contre-courant des aspirations légitimes des personnes souhaitant conserver la maîtrise de leurs données.

A cet égard, le renforcement des droits des personnes est l'un des axes majeurs du Règlement. Le législateur européen rappelle que L'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. L'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière importante. Les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère

personnel comme jamais auparavant dans le cadre de leurs activités (…) Les technologies ont transformé à la fois l'économie et les rapports sociaux (considérant 6). Il souligne ainsi que ces évolutions requièrent un cadre de protection des données solide (…) assorti d'une application rigoureuse des règles, car il importe de susciter la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur. Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant. (considérant 7). Le législateur européen regrette, enfin, que la directive 95/46/CE n'ait pas permis d'éviter le sentiment, largement répandu dans le public, que des risques importants pour la protection des personnes physiques subsistent, en particulier en ce qui concerne l'environnement en ligne. (considérant 9).

La formation restreinte considère, ainsi, au regard de l'ampleur des traitements déployés et de la nécessité impérieuse pour les utilisateurs de garder la maîtrise de leurs données, que ceux-ci doivent être mis en situation d'être suffisamment informés de la portée des traitements mis en œuvre et d'y consentir valablement, sauf à priver de base la confiance dans l'écosystème numérique.

En quatrième lieu, la formation restreinte tient à souligner que les manquements doivent être mis en perspective au regard du modèle économique de la société, en particulier de la place du traitement des données des utilisateurs à des fins publicitaires via le système d'exploitation Android. Compte tenu des avantages qu'elle retire de ces traitements, la société doit apporter une attention toute particulière à la responsabilité qui lui incombe au titre du RGPD dans leur mise en œuvre.

Il résulte de tout ce qui précède et des critères dont il a été dûment tenu compte par la formation restreinte, au vu du montant maximum encouru établi sur la base de 4% du chiffre d'affaires indiqué au point 2 de la présente décision, qu'une sanction pécuniaire est justifiée à hauteur de 50 millions d'euros, ainsi qu'une sanction complémentaire de publicité pour les mêmes motifs.

Il est également tenu compte de la place prépondérante occupée par la société sur le marché des systèmes d'exploitation, de la gravité des manquements et de l'intérêt que représente la présente décision pour l'information du public, dans la détermination de la durée de sa publication.

PAR CES MOTIFS

La formation restreinte de la CNIL, après en avoir délibéré, décide :

de prononcer à l'encontre de la société Google LLC, une sanction pécuniaire d'un montant de 50 (cinquante) millions d'euros ;

d'adresser cette décision à la société Google France Sarl en vue de l'exécution de cette décision ;

de rendre publique sa délibération, sur le site de la CNIL et sur le site de Légifrance, qui sera anonymisée à l'expiration d'un délai de deux ans à compter de sa publication.

Le Président

Jean-François CARREZ

Cette décision peut faire l'objet d'un recours devant le Conseil d'Etat dans un délai de quatre mois à compter de sa notification.

Analyse prédictive et personnalité

Jeoffrey SABBAH

Docteur en droit
Enseignant contractuel, Université de Bourgogne

Un changement d'ère…. – L'évolution des technologies de la communication a entraîné notre société dans une consommation excessive d'information[143]. Elle en est dépendante, voire fanatique, à tel point que *l'homo numericus* est né, balayant l'époque contemporaine pour s'installer dans l'ère numérique. Les outils informatiques sont de plus en plus performants et accompagnent l'homme dans toutes les tâches qu'il effectue, à l'instar des *weareable* et des applications qui y sont attachées – GPS, podomètre, mesure cardiaque, calendrier, calcul de calories absorbées et brûlées, *etc.* La technologie, qui agit comme une prothèse numérique, crée un humain numérique « augmenté » dont les capacités sont étudiées, voire améliorées [144]. Un véritable guide comportemental est instauré allant, depuis peu, avec la démocratisation des algorithmes prédictifs, jusqu'à ménager le travail intellectuel menant à la prise de décision.

Le fonctionnement des algorithmes prédictifs.- La prédictivité est un outil informatique récent, qualifié par certains de boule de cristal 2.0[145]. Elle modifie les habitudes sociales. Le droit ne peut l'ignorer, il doit être adapté et enrichir ses différents domaines des problématiques liées à l'utilisation de cette nouvelle technologie. Faut-il encore que le juriste se familiarise avec le

[143] Lire notamment : P. SIRINELLI et S. PREVOST, Noël 3.0, *D. IP/IT* 2018, p. 653.

[144] C. TORRES, « 3 QUESTIONS - L'Internet des objets bouleverse le droit de la protection des données personnelles », *JCP E*, n° 26, 25 Juin 2015, 528.

[145] M. BOUTEILLE-BRIGANT, « Intelligence artificielle et droit : entre tentation d'une personne juridique du troisième type et avènement d'un « transjuridisme » », *LPA* 2018, 62, p.7 ; F. ROUVIERE, « La justice prédictive, version moderne de la boule de cristal », *RTD Civ.* 2017 p.527; P. SIRINELLI et S. PREVOST, « Madame Irma, Magistrat », *Dalloz IP/IT* 2017, p. 557.

fonctionnement même des algorithmes prédictifs. Ces derniers sont un instrument de prévision fonctionnant par le traitement et l'analyse d'une grande masse de données. Ainsi, un système algorithmique « *combine les informations les plus diverses pour produire une grande variété de résultats : simuler l'évolution de la propagation de la grippe en hiver, recommander des livres à des clients sur la base des choix déjà effectués par d'autres clients, comparer des images numériques de visages ou d'empreintes digitales, piloter de façon autonome des automobiles ou des sondes spatiales, etc.* »[146]. En outre, « *certains algorithmes, dits auto-apprenants, voient leur comportement évoluer dans le temps selon les données fournies* »[147]. La construction d'un système algorithmique repose donc sur deux aspects[148]. D'une part, une grande quantité de données doit être mise en corrélation pour déduire les conséquences résultant d'un type de situation, d'autre part, la masse de données ne doit occulter la qualité de l'information, afin d'observer que les caractéristiques spécifiques – âge des personnes concernées, spécialité de l'avocat, type d'aliments … – d'une situation ont produit un résultat déterminé[149]. La justice prédictive illustre parfaitement l'usage actuel de cette technologie. Elle « *se compose d'un ensemble d'algorithmes permettant d'analyser des données juridiques et factuelles (textes, décisions, doctrines, faits…)* » [150] dans le but d'anticiper une décision de justice.

Algorithmes et droit de la personnalité.- Cependant, l'utilisation des systèmes algorithmiques n'est pas sans inquiéter. Les récentes révélations d'écoutes clandestines d'*Amazon*, par le biais des enceintes connectées *Alexa*[151], illustrent parfaitement ces propos. Les utilisateurs se sentent épiés et atteints dans leur sphère privée. Or, nombreux sont les droits garantissant l'intégrité de la personne et le respect de leur vie privée. Au demeurant, il ne

[146] Définition proposée par la CNIL : https://www.cnil.fr/fr/definition/algorithme

[147] C.E. Puissance publique et plateformes numériques : accompagner l'« uberisation » : rapp. annuel 2017 : http://www.conseil-etat.fr/Decisions-Avis-Publications/Etudes-Publications/Rapports-Etudes/Etude-annuelle-2017-Puissance-publique-et-plateformes-numeriques-accompagner-l-uberisation.

[148] L.-M. AUGAGNEUR, « D'où jugez-vous », *JCP G* 2018, p. 431.

[149] *Ibid.*

[150] M. MEKKI, "If code is law, then code is justice ? Droit et algorithmes, » *Gaz. Pal.,* juin 2017, n° 24, p. 10.

[151] E. BRAUN, Les utilisateurs d'Alexa sur écoute: un flou juridique inquiétant, Le Figaro, http://www.lefigaro.fr/secteur/high-tech/amazon-ecoute-les-utilisateurs-de-son-assistant-vocal-alexa-20190411 ; Auteur anonyme, Amazon écoute et analyse vos conversations pour améliorer son assistant vocal Alexa, Le 20 minute, https://www.20minutes.fr/high-tech/2494627-20190411-amazon-ecoute-analyse-conversations-ameliorer-assistant-vocal-alexa.

faut pas omettre que les systèmes algorithmiques sont composés de données personnelles. Leur fonctionnement impliquant des traitements massifs de données ne peut, par conséquent, s'effectuer librement. Les concepteurs et les responsables des traitements de données doivent mesurer les conséquences pratiques et juridiques des systèmes qu'ils instaurent dès leur création. Au demeurant, l'opinion publique montre du doigt le fameux « vide juridique », mal récurent de notre société, dont profite outrageusement les géants du GAFAM[152].

Par ailleurs, un usage aveugle de la prédictivité a pour risque de conduire à une déresponsabilisation de l'utilisateur. En effet, nombreux sont les domaines pouvant utiliser la prédictivité comme la médecine, la justice, la sécurité ou encore les ressources humaines. Les décisions prises en la matière sont importantes : détecter de potentiels auteurs d'infractions graves, prédire le succès d'une action en justice ou encore deviner des diagnostics à délivrer. Si le choix final découle d'une prise de décision humaine, il est impossible de quantifier la mesure dans laquelle l'utilisateur a agi librement, sans aucune influence du résultat proposé par le programme.

Or, nous pouvons craindre que les logiciels d'assistance prédictive incitent leurs utilisateurs à prendre des décisions dont les conséquences sont la violation des droits de la personnalité. Un algorithme relatif à la sécurité et à la commission d'infraction risque d'aller à l'encontre du principe de non-discrimination en stigmatisant des groupes de personnes habitant des quartiers défavorisés et plus enclins à la délinquance[153]. C'est de cette manière que le logiciel de reconnaissance faciale de Google a identifié en 2015, un homme

[152] L'acronyme désignant les géants du Web : Google, Apple, Facebook, Amazon et Microsoft.

[153] La police de Chicago utilise par exemple un programme d'algorithmes prédictifs pour lutter contre la criminalité et les fusillades régulières, voire quotidiennes. Lire notamment : J. CONTE, « Algorithme idéologique », *Dr. Pén.* 2017, n° 11, rep. 10 ; E. G. FERGUSSON, The Police Are Using Computer Algorithms to Tell If You're a Threat, 3 oct. 2017, *Time,* disponible à l'adresse suivante : http://time.com/4966125/police-departments-algorithms-chicago/

afro-américain en la forme d'un gorille[154]. Il est ainsi aisé d'y percevoir une violation de l'article 9 du Code civil, matrice des droits de la personnalité[155].

Les services et outils du numérique utilisant des algorithmes prédictifs sont donc considérables et, à l'exemple de chaque particularité et nouveauté technologique, découlent des risques concernant la personnalité de leurs utilisateurs.

Il est dès lors nécessaire d'orienter la réflexion sur les moyens juridiques dont ils disposent pour se protéger, ainsi que sur l'efficacité des normes applicables à l'utilisation d'algorithmes prédictifs, notamment lorsqu'il en résulte des atteintes aux droits de la personnalité. Les utilisateurs des technologies qui fonctionnent avec des systèmes prédictifs ne sont pas démunis face aux potentielles violations de leur vie privée. Le législateur les a pourvus d'outils juridiques qui leur permettent de se protéger contre toute numérisation intempestive de leur personnalité **(I)**. Toutefois, il est légitime de se demander si les normes en la matière sont effectives **(II)**.

I) Les outils juridiques au service de la prédictivité

L'analyse prédictive est largement exploitée par de nombreux services de la société du numérique. Ses acteurs économiques se servent d'algorithmes prédictifs, afin de profiler les utilisateurs d'internet et en tirer des profits. Ils brassent de nombreuses données à caractère personnel protégées par des normes spécifiques, lesquelles régulent également, dans cette hypothèse, les systèmes algorithmiques **(A)**. Cependant, leur application n'est pas sans difficulté **(B)**.

---

[154] http://www.leparisien.fr/high-tech/deux-afro-americains-confondus-avec-des-gorilles-google-s-excuse-02-07-2015-4912669.php ; Rapport CNIL, préc. p. 32

[155] P. JOURDAIN, « les droits de la personnalité à la recherche d'un modèle : la responsabilité civile », *Gaz. Pal.,* Avr. 2007, n° 139 ; A. LEPAGE, « l'article 9 du Code civil peut-il constituer durablement la « matrice » des droits de la personnalité ? », *Gaz. Pal.,* mai 2007, n° 139, p.43 ; A. MARAIS, *Droit des personnes*, 3e édit. Dalloz, Paris, 2018, p.197, 276 ; L. MARINO, « les nouveaux territoires des droits de la personnalité », *Gaz. Pal*., 19 mai 2007, n° 139, p. 22 ; J.- C. SAINT-PAU, « l'article 9 du Code civil : matrice des droits de la personnalité », *D.* 1999, p. 541.

A) Les normes régulant l'utilisation d'algorithmes

Algorithmes et données personnelles.- S'il est vrai que les règles encadrant l'utilisation d'algorithmes sont éparses, il est logique de se tourner vers celles relatives aux données personnelles et à la vie privée lorsqu'est en jeu la protection de la personne concernée. Encore faut-il démontrer que le fonctionnement des systèmes algorithmiques dépend de traitements de données à caractère personnel. L'emploi d'algorithmes prédictifs implique nécessairement une exploitation massive de données. Rappelons-le, selon la loi dite informatique et libertés[156] constitue une donnée à caractère personnel « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, […]* ». Le Règlement (UE) 2016/679[157] précise ; « *[…] notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* »[158]. Ces deux principaux textes apportent une définition large de la notion, dans laquelle il est simple d'y inclure les informations utilisées par les algorithmes prédictifs. En effet, si chacune d'elles prise isolément peut sembler anodine, leur croisement, afin d'obtenir des analyses statistiques fiables, amène à l'identification des utilisateurs.

L'application de ces normes exige également que les données personnelles fassent l'objet d'un traitement, c'est-à-dire de « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ». L'analyse statistique de données personnelles

[156] Art. 2 al. 1 loi informatique et libertés.
[157] Ci-après RGPD
[158] RGPD, art. 4.1 RGPD

est un traitement. Dès lors, c'est conformément aux normes relatives aux données personnelles que doivent être régulés bon nombre de systèmes algorithmiques, bien davantage que les autres normes juridiques composant les droits de la personnalité.

L'exemple des moteurs de recherches.- Le service que nous pouvons évoquer, pour illustrer nos propos, est le moteur de recherche *Google* de la société éponyme, lequel joue un rôle primordial dans le fonctionnement d'internet, puisqu'il est le premier point de contact de l'internaute pour accéder à une information[159]. Il est une catégorie de services de la société de l'information dont la finalité est de faciliter la recherche de données sur internet et de la rendre disponible de manière spécifique[160]. Dans ce but, un moteur de recherche traite toutes les données contenues sur internet, y compris les informations personnelles. L'utilisation des robots d'indexation archive une partie du web et, selon la requête de l'utilisateur, le moteur de recherche met en corrélation les informations pertinentes pour proposer une réponse à l'internaute. Partant, il est facile d'accéder à des éléments de sa vie privée. Un employeur « curieux » pourra aisément accéder à ceux de salariés potentiels en le « *googlisant* »[161], afin de vérifier *a minima* les compétences. Dans cette hypothèse des données personnelles sont traitées. La personne concernée est identifiée par la réunion d'attributs de sa personnalité comme un nom, une photographie, des compétences et même des relations privées et professionnelles.

Or, la société *Google* a amélioré son moteur de recherche par l'utilisation d'un algorithme prédictif, notamment avec le service *Google Suggest*.

Le service google suggest.- Il s'agit d'une fonctionnalité de recherche « suggestive », dont l'utilisation consiste à proposer une suite de mots-clés.

[159] G29, Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche, 4 avr. 2004, p. 8.

[160] P.-J. BENGHOZI, *Les moteurs de recherche : Trou noir de la régulation in Google et les nouveaux services en ligne - impact sur l'économie du contenu et questions de propriété intellectuelle*, (dir. A. STROWEL et J.-P. TRIAILLE), Larcier, Bruxelles, 2008, p. 84.

[161] Néologisme utilisé pour désigner la recherche d'informations sur une personne ou sur une chose à l'aide du moteur de recherche *Google*.

Celle-ci est présentée selon les éléments de recherche entrés par l'internaute[162]. Si l'internaute entre le mot « droit », *Google suggest* pourra afficher « droit au chômage ». La société Google propose à ses utilisateurs une aide supplémentaire dans leurs recherches sous la forme d'une saisie semi-automatique grâce à des algorithmes prédictifs. Le service de recherches associées suggère non seulement à l'internaute au début de sa frappe le mot entier[163], mais associe également, et de manière automatique, un terme à la requête de l'utilisateur. Les suggestions correspondent aux requêtes les plus pertinentes émises par les internautes et dépendent de la récurrence des recherches associées[164]. Ce mécanisme fonctionne également si la frappe de l'internaute correspond au nom d'une personne ou au signe distinctif d'une personne morale. Or, l'association entre la recherche par un élément d'identification et la suggestion proposée est parfois péjorative, voire préjudiciable. À la recherche « Max Mos », *Google suggest* a proposé « Max Mosley Nazi »[165], ou encore à la recherche « Direct énergie », *Google suggest* a suggéré « Direct énergie arnaque »[166]. Aussi, la fonctionnalité *Google suggest* crée-t-elle, dans cette hypothèse, un « profil public péjoratif ». Dès lors que l'internaute valide sa recherche suggérée, il accède à tout type d'informations telles que des articles, des images[167] ou des vidéos en rapport direct avec les termes peu flatteurs quasi imposés par le moteur de recherche[168]. L'internaute aurait-il lui-même imaginé cette recherche si elle n'avait pas été suggérée de la

[162] M. BOIZARD, « Les moteurs de recherche »*, in Lamy droit de la responsabilité*, mise à jour sept. 2013, étude 420- 90.

[163] J. HUET et E. DREYER, *Droit de la communication numérique*, L.G.D.J., Issy-Les-Moulineaux, 2011, p. 332, 351.

[164] D. CHALLAMEL, « Moteur de recherche - *Google suggest* : vers un épilogue judiciaire », *Expertises*, nov. 2013, p. 393 ; A. LEPAGE, « Google *suggest* : loi du 29 juillet 1881 écartée, responsabilité civile de droit commun sollicitée », *Comm. com. électr*., n°1, janvier 2014, comm. 10, p.43.

[165] Max MOSLEY est le président de la Fédération internationale de l'automobile.

[166] V. notamment CA Paris, Pôle 1, ch. 2, 9 déc. 2009, Google Inc. c. Direct Energie, note J. HUET, *Légipresse*, n°278, 1 déc. 2010, p. 426-430 ; TGI Paris, 8 sept. 2010 P. Bellanger c. Google Inc., *D.* 2010, p. 2356, obs. C. MANARA, TGI Paris, 17e ch., 31 oct. 2012, Antonio M. c. Google inc., obs. A. LEPAGE, *Comm. Com. électr.,* n°4 avr. 2013, comm. 46, p. 42 ; Cass. civ. 1er, 19 fév. 2013, M. X c. Google inc. n°12- 12798 ; TGI Paris 17e ch., 23 oct. 2013, Bruno L. et Ressource et actualisation c. Google inc. et Google France, obs. A. LEPAGE, *Comm. com. électr.,* janv. 2014, comm. 10, p. 43.

[167] V. TGI Paris 17e ch., 6 nov. 2013, Max Mosley c. Google France, Google inc., obs. L. COSTES, *RLDI,* n°99, déc. 2013, 3296, p. 42-43.

[168] C'est l'exemple de Max MOSLEY dont des vidéos, à caractère pornographique, de lui déguisé en officier nazi ont été diffusées.

sorte ? Pour réparer le préjudice qui en résulte, la Cour de cassation raisonne par le droit commun de la responsabilité civile[169].

Pourtant, ces profils péjoratifs portent atteinte aux droits de la personnalité. En effet, si ces droits étaient à l'origine compris comme la protection de la sphère d'intimité, notamment à travers le droit au respect à la vie privée, ils sont aujourd'hui appréhendés de manière large. Ils protègent l'autonomie de la personne et la préserve de toute surveillance abusive de la société[170]. En outre, ils lui octroient un droit de contrôle sur l'information qu'elle veut communiquer[171]. L'affaire Max Mosley révèle cette perte de contrôle de l'information due aux algorithmes de *Google suggest.* Agir sur le fondement de ces droits est préférable dans la mesure où la seule constatation de l'atteinte ouvre droit à réparation[172]. Au demeurant, ces droits peuvent s'exercer à l'écart de tout litige[173], à l'exemple du droit à l'image ou des droits relatifs aux données personnelles, comme le droit à l'oubli[174].

Algorithmes et autres normes.- Outre les normes régulant les données personnelles, il existe d'autres dispositions légales qui cantonnent l'utilisation d'algorithmes au respect de la personnalité. L'article 9 du Code civil a été rédigé dans l'objectif de protéger la sphère d'intimité des personnes. Néanmoins, dans un arrêt décisif[175] du 5 novembre 1996[176] la Cour de cassation constate l'autonomie de l'article 9 du Code civil érigeant ce dernier en matrice

[169] D. CHALLAMEL, *loc.cit* ; TGI Paris 17e ch., 23 oct. 2013, Bruno L., Ressources et actualisation c. Google inc., Google France., obs. J. DE ROMANET, *RLDI*, n°99, déc. 2013, 3297, p. 44-45.

[170] G. LOISEAU, *Les métamorphoses de la protection de la vie privée à l'heure du numérique*, Légipresse, 2011, p. 345 ; P. MALAURIE et A. AYNES, *Droits des personnes, la protection des mineurs et des majeurs*, 10e édit., LGDJ, Issy-Les-Moulineaux, 2018, p. 158, 312.

[171] D. GUTMANN, *Le sentiment d'identité – Étude de droit des personnes et de la famille*, LGDJ, Issy-les-Moulineaux, 2000, p. 222, 250 ; J. SABBAH, *Contribution à l'étude de la personnalité à l'ère numérique*, thèse Strasbourg, soutenue 2018, p. 411, 401.

[172] Cass. 1er civ., 5 nov. 1996, Bull. n° 378, p. 265.

[173] J.- C. SAINT-PAU, « Le droit au respect à la vie privée » *in Traités – Droits de la personnalité* (dir. J.-C. SAINT-PAU), LexisNexis, Paris, 2013, p.269, 438.

[174] *Ibid*.

[175] D'autres décisions seront par la suite rendues en ce sens pour d'autres droits de la personnalité que le droit au respect à la vie privée. V. par exemple : Cass. 1er civ., 25 fév 1997, Mme Mebon c. époux Bauzon, note J. RAVANAS, *JCP G*, 1997, n° 27, II, 22873.

[176] Cass. 1ère civ., 5 nov. 1996, SNC Prisma Presse c. Mme G., n° 94-14798 ; obs. J. HAUSER, « La protection de la vie privée : conditions et sanctions », *RTD Civ*. 1997 p.632 ; J. RAVANAS, « L'article 9 du Code civil ouvre-t-il un droit à réparation autonome » *JCP G*, 19 Mars 1997, n° 12, II, 22805 ; G. VINEY, préc., I, 402 ; J.- C. SAINT-PAU, préc., 18.

des droits de la personnalité et élevant le droit au respect à la vie privée en une notion-cadre[177]. Ainsi ce dernier est-il compris de manière large, voire extensive, au point que « *le droit au respect de la vie privée a vocation à absorber tous les droits de la personnalité ayant pour objet de protéger l'intégrité morale* »[178]. À l'unité de la personnalité correspond l'unité du droit qui la préserve[179]. L'article 9 doit être envisagé comme un droit « de contrôle », qui se compose du droit de « contrôler sa vie privée »[180]. Il est également le pivot de l'individualisation de la personne par son identification effective ou possible[181]. En maîtrisant ce que l'on dévoile de sa personne, on protège indirectement chacun des attributs de sa personnalité. Par conséquent, les algorithmes prédictifs, et plus précisément ceux dont les résultats profilent l'utilisateur, ne peuvent porter atteinte à la personnalité et au droit au respect à la vie privée en vertu de l'article 9 du Code civil. Dès lors, et face aux algorithmes, la protection de la personnalité réside principalement dans l'application des dispositions du RGPD et de la loi informatique et libertés modifiée par la loi du 20 juin 2018 relative à la protection des données personnelles[182], comme le rappelle respectivement leur article premier. Les objectifs fixés sont la protection de la personnalité à l'égard du traitement des données à caractère personnel, la sauvegarde des libertés et droits fondamentaux des personnes physiques et en particulier leur droit à la protection des données personnelles[183]. Dans cette perspective, « *l'informatique doit être au service de chaque citoyen. […]. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* »[184]. Ce n'est donc pas en terme de vide juridique qu'il convient d'élaborer de nouveaux droits. Ceux existants sont

[177] J.-M. BRUGUIERE et B. GLEIZE, *Droit de la personnalité*, Ellipse, Paris, 2015, p. 138, 151.
[178] J.- C. SAINT-PAU, « L'article 9 du Code civil : matrice des droits de la personnalité », préc., p. 541.
[179] J.-M. BRUGUIERE, « Dans la famille des droits de la personnalité, je voudrais…. », préc., p. 28, 2 ; L. MARINO, « Les nouveaux territoires des droits de la personnalité », *Gaz.Pal*. 19 mai 2007, n° 139, p. 22 ; J.- C. SAINT-PAU, *loc.cit.*
[180] D. GUTMANN, *op. cit.*, p. 340, 408 ; A. LEPAGE, « L'article 9 du Code civil peut-il constituer durablement la « matrice » des droits de la personnalité ? », préc., p.43 ; L. MARINO, « Les nouveaux territoires des droits de la personnalité », préc., p. 22.
[181] A. LEPAGE, *loc.cit*.
[182] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (1), *JORF* n°0141 du 21 juin 2018 texte n° 1
[183] RGPD art. 1
[184] Loi informatique et libertés art. 1 al. 1

suffisants. Légiférer sur une technologie aussi moderne que les algorithmes pourrait imposer des règles inadaptées et rapidement caduques.

B) Les algorithmes prédictifs à l'épreuve du droit

Les assistants vocaux et la vie privée. – Dernier service proposé à ce jour par les sociétés du numérique : les assistants vocaux. Ces derniers ne sont pas sans poser de questions plus précisément concernant leur fonctionnement à l'égard de la vie privée. La voix de l'utilisateur est numérisée et sollicitée comme une interface d'interaction utile au fonctionnement de ces nouveaux services[185]. Ces derniers sont des applications fonctionnant grâce à un programme d'intelligence artificielle qui analyse les habitudes de leurs utilisateurs et répondent à des requêtes formulées oralement, ainsi qu'à l'aide d'analyse prédictive comportementale.

Les assistants vocaux ont d'abord été développés sur les *smartphones*, l'assistant le plus connu étant *SIRI*. Puis, ils ont été déployés sur d'autres appareils suite à l'avènement des objets connectés[186]. Ils rencontrent aujourd'hui un franc succès commercial avec les enceintes connectées à l'instar d'*Alexa* et de *Google Home*. Équipées d'un haut-parleur et d'un microphone, elles sont capables d'interagir avec l'utilisateur et de l'assister en lui donnant la météo, en activant ses lumières, en lisant ses courriels ou encore en lui permettant d'effectuer des achats en ligne. Ces objets domotiques fonctionnent en cinq étapes,[187] dont une préliminaire. D'abord, l'utilisateur configure l'appareil. Pour cela, il communique un certain nombre de données, dont sa voix qui est enregistrée et analysée afin d'optimiser les performances de l'assistant vocal. Puis, l'internaute « réveille » la machine grâce à une expression clé – « *ok Google* » ou encore « *Alexa ?* » – et communique sa demande par oral. La requête énoncée est ensuite enregistrée, ce qui implique une collecte de données, la création d'un historique, voire son enregistrement dans le *Cloud*. Les paroles prononcées sont transcrites en données, après quoi la machine répond. Enfin, l'assistant retourne en veille. Il est évident qu'un tel

[185] O. DESBIEY, « Ok Google et Siri ne suivent pas la même voie qu'Alexa ou Cortana », 27 mars 2018, disponible sur : https://linc.cnil.fr/fr/ok-google-et-siri-ne-suivent-pas-la-meme-voie-qualexa-ou-cortana

[186] À l'exemple des casques, habitacles de voiture et autres.

[187] CNIL, Enceintes intelligentes : des assistants vocaux connectés à votre vie privée, 5 déc. 2017, https://www.cnil.fr/fr/enceintes-intelligentes-des-assistants-vocaux-connectes-votre-vie-privee

fonctionnement affecte la vie privée de l'utilisateur. On s'interroge, par exemple, sur ce qu'il advient des paroles prononcées. Elles ne s'effacent pas, comme disparaissent les mots d'une conversation tenue de vive voix. Elles restent dans les serveurs de la même manière que si l'internaute avait formulé sa requête à l'aide d'un clavier sur un moteur de recherche, ce dont il n'a pas nécessairement conscience. *Quid*, également, de l'analyse des propos portés à la machine et de ceux interceptés clandestinement ? Qu'en est-il du droit au respect de la vie privée du groupe d'utilisateurs, dans la mesure où l'assistant enregistre les voix d'un foyer et non d'un seul utilisateur – c'est l'hypothèse de l'enceinte connectée – et de celle des personnes tierces qu'il peut entendre ? Enfin, comment régler juridiquement les risques liés au fonctionnement même de la machine et aux piratages possibles[188]. Si l'assistant vocal interprète mal une donnée ou s'il est « trompé », un faux consentement peut être recueilli et former une sorte de violation de ses données par l'entremise d'un tiers.

Les principes indispensables à la protection de la personnalité.- Le RGPD et la loi informatique et libertés apportent des solutions convenables à ces problématiques. Les normes relatives aux données personnelles imposent aux responsables de traitement de respecter de grands principes indispensables à la protection de la personnalité dans ses activités numériques. Il convient d'exposer, tout d'abord, les exigences de consentement de la personne concernée, de traitement loyal, licite et transparent des données, de leur portabilité ou encore de leur effacement. En d'autres termes, la personne concernée exerce un droit de regard, voire un droit de contrôle sur ses données, qui peut s'interpréter comme une réappropriation et une autodétermination informationnelle[189]. Ainsi est-il juridiquement impossible pour le responsable de traitement d'enregistrer des voix, quelle que soit la raison[190], lorsque l'enceinte connectée est en veille et sans que l'utilisateur ne la sollicite.

[188] Lire notamment : C. S. SMITH, "Alexa and Siri Can Hear This Hidden Command. You Can't", New York Times, 10 mai 2018, https://www.nytimes.com/2018/05/10/technology/alexa-siri-hidden-command-audio-attacks.html

[189] Lire notamment : J. ROCHFELD, « La vie tracée ou le Code civil doit-il protéger la présence numérique des personnes » *in* mélanges en l'honneur du Professeur Jean Hauser, Dalloz, Paris 2012, p. 636, 16.

[190] Y compris celle d'améliorer ses algorithmes d'analyse de requête comme pour l'enceinte Alexa.

De surcroît, le RGPD impose le respect en amont de concepts, à l'exemple de l'*accountability*[191] ou encore, en son article 25, du *privacy by design*[192]. Ce dernier consacre à la charge des concepteurs et des responsables de traitement résultant d'algorithmes une obligation préventive de mettre en œuvre toutes mesures techniques adaptées à la protection des données de l'utilisateur. Il s'agit, avant tout, de mettre en forme toutes les possibilités permettant l'anonymisation et la pseudonymisation des données collectées. Au demeurant, la violation de ce principe est sanctionnée, selon l'article 83.4 du RGPD, d'une amende administrative élevée[193] et suffisamment contraignante pour les acteurs du secteur[194]. Il est également question de s'assurer que le produit aboutissant à un traitement de données est, dès sa conception, conforme aux principes du RGPD. Les inventeurs d'enceintes connectées doivent s'assurer qu'en aucun cas le fonctionnement de la machine ne porte atteinte aux droits de la personnalité, même si elle se déclenche, par exemple, accidentellement[195].

Il faut enfin évoquer, au vu de l'importante place que prend la justice prédictive, notamment par l'usage des *legaltechs*, l'interdiction de décisions de justice impliquant une appréciation sur le comportement d'une personne ou de décisions ayant des effets juridiques à l'égard des personnes concernées, fondées exclusivement sur un traitement de données automatisées, c'est-à-dire qu'une machine peut prendre seule sans intervention humaine[196]. Ainsi, le responsable du traitement ou celui qui tire les conséquences des résultats proposés par la machine ne peut se contenter de les suivre. Il doit effectuer un

[191] L'accountability désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données. https://www.cnil.fr/fr/definition/accountability

[192] Voire du *Privacy by Using*. Lire notamment : S. BERNHEIM-DESVAUX, M. FAVREAU, V. NICOLAS, J. SENECHAL et C. ZOLYNSKI, » La consommation d'objets connectés, un marché économique d'avenir », *CCC* 2018, n° 7, étu. 9.

[193] « Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu ».

[194] C. ZOLYNSKI, « La *Privacy by Design* appliquée aux Objets Connectés : vers une régulation efficiente du risque informationnel ? », *Dalloz IP/IT* 2016, p.404.

[195] La société Snips apporte un bon exemple. Elle a créé une enceinte qui respecte entièrement la vie privée car la voix est analysée directement dans l'objet auquel l'utilisateur s'adresse, sans qu'aucune donnée ne soit envoyée dans le cloud. Lire à ce propos A. MORA, « Snips, l'assistant vocal qui respecte votre vie privée », Capital, 3 juill. 2018, https://www.capital.fr/votre-carriere/snips-lassistant-vocal-qui-respecte-votre-vie-privee-1296037

[196] Lire RGPD art. 22 et article 10 loi informatique et libertés.

travail d'interprétation l'empêchant par conséquent, en cas d'erreur, de se déresponsabiliser.

II) L'efficacité des outils juridiques au service de la prédiction

Mesurer l'efficacité des outils juridiques qui protègent les utilisateurs des analyses prédictives nécessite de s'intéresser à l'effectivité des normes en la matière **(A)** et à soulever l'existence de limites techniques **(B)**.

A) L'effectivité des normes

L'effectivité des différents principes.- Il est, en premier lieu, possible de s'interroger sur l'effectivité de ces différentes normes. Plusieurs failles peuvent être soulevées. Tout d'abord, les solutions qu'apportent le RGPD ou la loi informatique et libertés ne fonctionnent que pour les algorithmes traitant des données à caractère personnel. Toutefois, beaucoup n'en utilisent pas, à l'exemple de ceux qui ont une fonction purement économique ou encore dont l'objectif est l'accompagnement d'achat et revente. Pour autant, ils peuvent avoir un impact sur la personne, notamment s'ils sont utilisés à grande échelle. L'exemple du *Healthy*[197] est significatif : il est simple d'imaginer un algorithme prévoyant les heures et compositions de repas selon le coût et la qualité nutritive des aliments, ainsi que le temps à consacrer aux activités intellectuelles et celui réservé pour la pratique du sport, selon une régulation en apports caloriques. Il est évident qu'un tel système aurait des répercussions socio-économiques sur l'utilisateur, voire sur un groupe de personnes, par une gestion différente de sa sphère d'intimité, ce qu'aucune norme n'a encore envisagé. Il nous semble que la justice prédictive et les *legaltechs* soulèvent les mêmes difficultés. Si leur but est bien d'accompagner les juristes, ne risquent-elles pas, en réalité, de les remplacer ? Bien que nous fassions pleinement confiance aux hommes de loi, la justice prédictive a pour danger de les enfermer dans des syllogismes formels, voire normatifs. Pour tel type de dommage doit être apportée telle solution, puisqu'elle est la plus rentable et la

[197] Terme utilisé pour désigner la tendance actuelle à s'approcher le plus près d'un mode de vie sain.

moins risquée. « *La justice prédictive ne doit pas devenir une justice déshumanisée* »[198].

Afin d'empêcher ces déviances, il faut s'assurer que l'homme intervienne systématiquement dans la prise de décision finale et qu'il ne se décharge pas entièrement de la tâche qui lui incombe, mais qu'il se déleste uniquement de sa pénibilité. Différentes solutions sont envisageables. À l'instar des cookies signalés à l'aide d'une bannière d'information préalable, une méthode équivalente peut être imposée pour prévenir les personnes concernées de l'utilisation de système d'algorithmes prédictifs. Les utilisateurs alors prévenus deviennent plus méfiants à l'égard du système, obligeant les concepteurs à être plus vigilants quant au respect des principes imposés par le RGPD et la loi informatique et libertés.

Concernant le fonctionnement des *legaltechs*, il semble opportun d'instaurer un devoir de prudence relatif à la prise de décisions qui découlent d'analyses prédictives. L'objectif est de ne pas rendre automatique la validation d'un résultat proposé par le programme utilisé, ce qui implique d'agir en amont. Par conséquent, il est logique que l'obligation se formalise par le respect de règles de conduite insérées dans les chartes informatiques des cabinets d'avocats.

Dans une pareille logique, ces normes ne prennent pas en compte les personnalités collectives[199]. Pourtant, de plus en plus d'outils fonctionnant avec des algorithmes prédictifs sont employés par plusieurs personnes, à l'instar des assistants vocaux. C'est pourquoi le nouvel article 43 *ter* de la loi informatique et libertés[200] prévoit une action de groupe qui peut s'exercer pour les personnes physiques qui ont subi un dommage ayant pour cause un manquement de même nature, à savoir la violation d'une disposition du RGPD[201]. Au demeurant, toute action de groupe peut être intentée devant les

[198] M. MEKKI, préc.

[199] J. SABBAH, *Contribution à l'étude des droits de la personnalité à l'ère numérique*, thèse Strasbourg, soutenue le 9 novembre 2018.

[200] Article 25 Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (1) *JORF* n°0141 du 21 juin 2018 texte n° 1.

[201] Art. 43 *ter* II loi informatique et libertés« *Lorsque plusieurs personnes physiques placées dans une situation similaire subissent un dommage ayant pour cause commune un manquement de même nature aux dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi par un responsable de traitement de données à caractère personnel ou un sous-traitant, une action de groupe*

juridictions civiles et administratives, afin de faire cesser le manquement invoqué ou pour obtenir réparation du préjudice[202].

Enfin, il faut admettre, comme le démontrent les bilans proposés par la CNIL, qu'il est complexe d'appliquer ces grands principes aux traitements de données personnelles[203]. Il est, *a fortiori*, plus difficile de les respecter lorsque les systèmes algorithmiques sont constitués de données dérivées qui découlent d'analyses d'informations[204], à l'instar des systèmes comme *Alpha Go*[205]. Ces derniers sont, dans une certaine mesure, autonomes et ont recours aux algorithmes d'apprentissages dont le contrôle des traitements devient complexe.

B) Les limites résultant de la technique

Les limites techniques.- En second lieu, il convient de soulever l'existence de limites techniques. Rappelons que pour répondre à ces difficultés, le RGPD a instauré l'obligation pour les concepteurs et responsables de traitement de

---

peut être exercée devant la juridiction civile ou la juridiction administrative compétente au vu des cas individuels présentés par le demandeur, qui en informe la Commission nationale de l'informatique et des libertés ».

[202] Voir art. 43 *Ter* III loi informatique et libertés.

[203] https://www.cnil.fr/fr/rgpd-quel-premier-bilan-4-mois-apres-son-entree-en-application; https://www.cnil.fr/fr/rgpd-quel-bilan-6-mois-apres-son-entree-en-application

[204] J.-M. DELTORN, « La protection des données personnelles face aux algorithmes prédictifs », *RDLF* 2017, chron. n°12, http://www.revuedlf.com/droit-ue/la-protection-des-donnees-personnelles-face-aux-algorithmes-predictifs/

[205] Il s'agit d'un programme pour jouer au Go, un jeu considéré comme plus complexe que les échecs. Il a gagné contre le champion du monde parce que son système est fondé sur l'apprentissage autonome (R. CHATILA, « Intelligence artificielle et robotique : un état des lieux en perspective avec le droit », *D. IP/IT* 2016, p.284 ; Rapport CNIL, préc. p. 16) – autrement appelé le *machine learning*. L'intelligence artificielle est constituée d'algorithmes prédictifs qui analysent de nombreuses situations identiques de sorte à obtenir la capacité d'apporter la meilleure solution possible lorsqu'elle se trouve dans un contexte identique La machine devient plus performante parce qu'elle acquiert une expérience en jouant contre l'homme. Récemment, une intelligence artificielle de Facebook a, d'elle-même inventé, son propre langage (http://mashable.france24.com/medias-sociaux/20170620-intelligence-artificielle-facebook-messenger-chatbots-langage). Les nouvelles intelligences artificielles font donc preuve d'une autonomie telle, qu'elles sont capables de prendre des initiatives sans aucune intervention humaine, ainsi que de prédire la meilleure solution à un état donné. L'homme perd le contrôle de sa machine (A. BENSAMOUN, « Des robots et du droit... », *Dalloz IP/IT* 2016, p.281 ; G. LOISEAU, « Des robots et des hommes », *D.* 2015, p.2369 ; R. CHATILA, *op.cit.*) qui atteint une maturité assez élevée pour se comporter quasiment comme lui. Des questions éthiques et juridiques se posent alors, notamment parce que leur fonctionnement dépend du traitement d'un nombre important de données – l'algorithme ne peut fonctionner s'il ne s'alimente pas de données – qui pour beaucoup sont personnelles.

respecter les principes de *privacy by design* ou encore *privacy by default*[206]. Ces derniers imposent que le traitement de données, ou l'outil informatique, soient conformes, dès leur création, aux dispositions du RGPD, ce qui passe notamment par des mécanismes de pseudonymisation et d'anonymisation des données. Ces mesures sont synonymes de progrès, mais elles ne sont pas infaillibles. Au demeurant, il existe de nombreuses techniques de désanonymisation, grâce au croisement d'informations et de données récupérées sur les serveurs. Certes, ces méthodes sont complexes. Pour autant, elles permettent d'affirmer qu'aucun responsable de traitement ne peut garantir d'anonymat absolu[207].

Par ailleurs, Il n'existe aucune garantie que les codes d'éthiques des algorithmes prédictifs ne soient pas modifiés par des tiers, voire par leurs concepteurs eux-mêmes[208].

Quid enfin, à l'égard des technologies comme les assistants vocaux, de la conscience de l'utilisateur du fonctionnement de la machine et, *a fortiori,* de l'obtention par le responsable du traitement de son consentement libre et éclairé relatif au traitement de données le concernant. Il ne peut, dès lors, exercer son « droit de curiosité »[209] et ainsi se voir informer de *« l'existence d'une prise de décision automatisée, y compris un profilage, [et des] conséquences prévues de ce traitement pour la personne concernée* » [210]. On ne peut affirmer, lorsque le microphone n'est pas éteint, que la machine n'écoute pas et n'effectue pas un traitement de tout ce qui est prononcé dans la pièce, même si elle reste en veille.

---

[206] Concernant ces notions, lire notamment : C. ZOLYNSKI, « La *Privacy by Design* appliquée aux Objets Connectés : vers une régulation efficiente du risque informationnel ?, » *Dalloz IP/IT* 2016, p.404 ; C. ZOLYNSKI, P. PUCHERAL, A. RALLET et F. ROCHELANDET, « La Privacy by design : une fausse bonne solution aux problèmes de protection des données personnelles soulevés par l'Open data et les objets connectés ? », *Légipresse* 2016, n° 340, p. 395-402.

[207] Lire notamment : F. CREUX-THOMAS, Technologies de l'information - « Les promesses d'une justice dite prédictive reposant sur des décisions de justice déjà rendues sont à tempérer (...) En quelque sorte, c'est le rétrospectif qui fait le prédictif ! » - Entretien par Loïc CADIET, Revue pratique de la prospective et de l'innovation n° 1, Avril 2018, entretien 2 ; J.-M. DELTORN, préc.

[208] J.-B. PREVOST, « Justice prédictive et dommage corporel : perspectives critiques », *Gaz. Pal.* 2018, n° 4, p. 43.

[209] Concernant l'idée de droit de curiosité lire notamment : M. BENEJAT, « Les droits sur les données personnelles *in* Traités – Droits de la personnalité » (dir. J.-C. SAINT-PAU), LexisNexis, Paris, 975, p.599 ; C. CASTET-RENARD, *Droit de l'internet : Droit français et européen*, Montchrestien, Paris, 2012, p. 44, 115 ; A. LUCAS, J. DEVEZE et J. FRAYSSINET, *Droit de l'Informatique et de l'internet*, PUF, Paris, 2001, p. 100, 150.

[210] Règlement UE 2016/679, art. 14 1. g)

Les services de streaming : un exemple de limitation technique. Le *streaming* est un service de plus en plus consommé par les internautes. Les applications de *streaming* analysent l'ensemble des visionnages des utilisateurs, en déduisent un genre musical ou de vidéo et recommandent à l'abonné une liste de musiques, de clips et de films correspondant à ses habitudes.

La maîtrise de ces algorithmes apporte à l'utilisateur un confort « intellectuel », afin de lui éviter des recherches infructueuses et le visionnage ou l'écoute d'œuvres déplaisantes pour lui, l'incitant à s'abonner à un autre prestataire[211].

Il est simple de constater, à travers ces incitations, un enfermement algorithmique très critiquable portant une atteinte à la personnalité de l'internaute ayant pour effet de nuire au pluralisme culturel[212]. L'algorithme prédictif cantonne l'individu dans une communauté culturelle conforme à ses propres goûts et crée un mur difficile à franchir, qui bloque l'accès à l'inconnu. Au demeurant, cette bulle culturelle n'est justifiée que par la rentabilité économique. Ainsi le développement personnel est-il réfréné par les intérêts de l'entreprise[213]. Un utilisateur curieux consultera naturellement divers types d'œuvres. L'information selon laquelle il a besoin de variété pour apprécier le service proposé sera envoyée, ce que le programme prédictif prendra en compte dans le calcul de ses suggestions. Il reste néanmoins que nous pouvons assimiler cette méthode à une ingérence injustifiée dans la construction de l'*alter ego* numérique, qui n'est dès lors plus libre, mais guidée, de sorte à la rendre économiquement plus rentable.

[211] Il est possible d'évoquer à ce propos le pourcentage proposé par Netflix qui indique à l'utilisateur les faibles ou fortes chances pour qu'il apprécie une œuvre. Ce calcul est effectué selon un algorithme qui prend en compte les visionnages déjà effectués par l'utilisateur.
[212] Rapport CNIL, Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle - synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une république numérique, déc. 2017, p. 35.
[213] *Ibid.*

L'optimisme.- Il est possible de proposer des pistes de réflexion pour combattre ces limites. La CNIL s'en est d'ailleurs saisie et propose une série de recommandations dont la première nous semble essentielle à une utilisation saine et sécuritaire de l'algorithme prédictif : la formation des citoyens, professionnels et concepteurs à l'éthique des « chaînes algorithmiques ». La loi ne peut-être le seul rempart face aux dangers de l'utilisation de systèmes algorithmiques. Une démarche pédagogique doit être entreprise par les institutions en charge de la protection des données personnelles. L'objectif est de fournir les clés de compréhension permettant d'aborder de manière confiante, active et éclairée ces nouvelles technologies[214]. Des temps doivent être dédiés à la sensibilisation de cette technologie, tant dans les universités que dans les milieux professionnels, par exemple, par le biais de formations obligatoires. Cette mesure doit être complétée par la maîtrise de l'utilisateur sur les chaînes d'algorithmes le concernant. Il est alors nécessaire de lui fournir des moyens techniques de contrôler et d'intervenir *ex ante, pendante* et *ex post*[215], sur la chaîne algorithmique. D'autres recommandations sont exposées à l'exemple de celle préconisant de « *travailler le design des systèmes algorithmiques au service de la liberté humaine* », mais elles semblent toutes être une application indirecte du *privacy by design* et du *privacy by default*. Une autre solution consiste en l'interdiction d'algorithmes dans les domaines trop sensibles, à l'instar des données personnelles visées à l'article 8 de la loi informatique et libertés dont le traitement est par principe impossible. Dans cette même logique, il serait opportun que la CNIL instaure une activité de certification de conformité au RGPD et à un usage éthique des données composant les algorithmes et l'intelligence artificielle.

Enfin, il paraît nécessaire d'imposer une obligation directe d'intervention humaine dans la création et l'utilisation d'algorithmes, qui se traduit, comme le démontre la CNIL, par le respect d'un impératif de vigilance[216]. Les systèmes algorithmiques, notamment avec le développement des *machines learning*, sont bien trop imprévisibles. L'homme ne peut se libérer de toute action sur cette technologie, sans craindre d'être exclu des prises de décisions pour

[214] Rapport CNIL, préc. 54.
[215] Voir notamment en ce sens, en matière de justice prédictive, M. MEKKI, préc.
[216] Rapport CNIL, préc., 50.

lesquelles le programme est, à la base, un simple assistant. La machine ne doit pas choisir à la place de l'homme, car toute situation ne saurait se résoudre convenablement par une simple analyse de données. Dans l'hypothèse d'un accident inévitable généré par une voiture autonome, le programme choisira très certainement d'éviter le plus de piétons, même s'il doit blesser un jeune enfant, alors que l'homme choisira, bien que cela soit moins rationnel, de préserver les plus jeunes au péril de sa propre vie…

Le cerveau et le droit

Adrien BOUVEL

Maître de conférences HDR à l'Université de Strasbourg
Chargé de cours à Sciences-Po Paris

Ce texte n'est pas une publication scientifique satisfaisant aux exigences du genre et, en particulier, à celle d'un appareil documentaire exhaustif. Il constitue plutôt un propos de candide, la réflexion naissante d'un scientifique, enseignant chercheur en droit, forcé d'admettre que la discipline qu'il pratique depuis près de trente ans connaît une crise profonde et qui, de façon peut-être un peu naïve, s'interroge sur des moyens susceptibles de l'atténuer quelque peu…

———————————

La loi, le système judiciaire, font l'objet de griefs constants, émanant tant des justiciables que des professionnels du droit.

L'opinion majoritairement défavorable des sujets de droit s'inscrit dans le mouvement actuel de défiance à l'égard des institutions ; elle ne doit assurément pas être négligée au motif qu'un non spécialiste ne serait pas à même d'émettre un avis pertinent sur la façon dont fonctionne un système aussi complexe. Le justiciable est le destinataire de la loi, des droits et devoirs qu'elle énonce, et le bénéficiaire du service public de la justice. La loi et la justice sont faites pour lui. Elles doivent avoir sa confiance, lui sembler légitimes. Or, nombre de nos contemporains reprochent à la norme d'être inintelligible, inadaptée, obsolète, pléthorique, dépendante du contexte politique, inefficace, inéquitable… En un mot comme en cent, imparfaite. Au système judiciaire, on oppose sa lenteur, son opacité, le coût des procédures,

les discriminations -réelles ou fantasmées- qu'il ferait entre le « vulgum » et les élites. Il s'agit de lieux communs, sans doute… Donc de croyances qui ne sont ni tout à fait exactes ni tout à fait erronées…

Le sentiment du professionnel du droit, praticien comme chercheur, n'est guère plus flatteur. Combien de spécialistes renommés confessent se sentir de plus en plus mal à l'aise dans une discipline qu'ils fréquentent pourtant depuis de nombreuses années, avouent éprouver la sensation désagréable de n'être plus en mesure de délivrer un conseil fiable à un client… De nombreux champs du droit sont décrits par des sommités sous un jour kafkaïen: inextricables, confus, contradictoires, incomplets, sans logique propre… Ce qui est pour le moins paradoxal à l'heure où l'on prône la simplification et l'harmonisation européenne du droit.

Pourquoi évoquer ces circonstances en introduction d'un article intitulé « Le cerveau et le droit » ? Simplement après avoir observé que de nombreuses disciplines scientifiques semblent s'enrichir -voire pour certaines se renouveler fondamentalement- sous l'effet d'enseignements tirés des découvertes les plus récentes réalisées dans le domaine des neurosciences, et plus particulièrement des neurosciences cognitives. Rares sont les secteurs dans lesquels celles-ci n'ont pas essaimé. En premier lieu, on songe bien entendu à la médecine[217], à la psychologie[218]. Mais des matières *a priori* plus lointaines comme les sciences de l'éducation[219], l'économie[220], le marketing, les ressources humaines, le management, la formation ou l'entrainement sportif[221], l'art[222],

[217] Dont les neurosciences sont devenues un champ disciplinaire à part entière.

[218] Les thérapies cognitives et comportementales s'inspirent très largement des travaux des neuroscientifiques. Le succès tant curatif que préventif des thérapies fondées sur la méditation, l'hypnose, la sophrologie, le yoga doit beaucoup aux neurosciences: ces pratiques sont anciennes, millénaires pour certaines d'entre elles, mais leur efficacité n'était jusqu'alors que constatée ; les neurosciences et, en particulier, les progrès très récents de l'imagerie cérébrale ont permis d'expliquer scientifiquement les raisons d'une telle efficacité, donnant ainsi à ces pratiques leurs lettres de noblesse et leur ouvrant même les portes des facultés de médecine.

[219] Voir, par exemple, J.-L. BERTHIER, G. BORST, M. DESNOS et F. GUILLERAY, *Les neurosciences cognitives dans la classe : Guide pour expérimenter et adapter ses pratiques pédagogiques*, ESF 2018, G. BORST et O. HOUDÉ, *Le cerveau et les apprentissages*, Nathan 2018, S. DEHAENE, *Apprendre à lire: Des sciences cognitives à la salle de classe*, Odile Jacob 2011, S. DEHAENE, *Apprendre ! : Les talents du cerveau, le défi des machine*, Odile Jacob 2018, S. DEHAENE, *La Bosse des maths: Quinze ans après*, Odile Jacob 2010, S. DEHAENE, *Les Neurones de la lecture*, Odile Jacob 2007, O. HOUDÉ, *L'école du cerveau : De Montessori, Freinet et Piaget aux sciences cognitives*, Mardaga 2018, J. STORDEUER, *Comprendre, apprendre, mémoriser : Les neurosciences au service de la pédagogie*, De Boeck 2014.

[220] C. SCHMIDT, *Neuroéconomie*, Odile Jacob 2010, S. GIRONDE, *La neuroéconomie*, Plon 2010.

[221] Z. SCHONBRUN, *Neurosciences et sport*, Amphora 2019.

l'architecture[223], l'histoire, la géographie, la science politique, les relations internationales et bien d'autres encore tirent profit de ce que les neurosciences apprennent de plus neuf sur le fonctionnement du système nerveux et cérébral, donc sur le comportement humain… A l'inverse, le droit -français comme européen[224]- fait preuve à leur égard d'une indifférence quasi totale[225], ce qui est particulièrement étrange d'une matière par nature au coeur des activités humaines et sociales. Là se situe le point de départ de notre réflexion.

Les travaux des neuroscientifiques sont abondants et variés. Depuis quelques années, ils connaissent une vogue populaire très nette qui offre un écho médiatique substantiel aux plus abordables ou novateurs d'entre eux. Rien de très surprenant puisque ces découvertes permettent de comprendre des comportements, réactions ou émotions humains, de les interpréter, voire de les modifier ou de les corriger. Elles permettent en outre d'expliquer des pratiques empiriquement observées de longue date, mais jusqu'alors qualifiées de croyances ou d'errances obscurantistes faute de recevoir la caution d'une explication scientifique rationnelle[226]. Puisque bon nombre de recherches en neurosciences sont relatives à des agissements ou des décisions de l'humain auxquels le droit lie des conséquences juridiques, il semblerait logique qu'il en tire conclusion tant dans la rédaction de la norme que dans son application, dès

[222] On peut à cet égard évoquer le travail de l'auteure, compositrice, interprète Barbara CARLOTTI, dont le dernier album « Magnétique » (Elektra 2018) a été intégralement conçu à partir d'idées, images, fragments de mélodies ou de textes apparus durant les phases de sommeil paradoxal. L'artiste s'est enfermée durant un mois dans une maison en Bretagne, et s'est obligée à se réveiller toutes les quatre-vingt-dix minutes afin d'y consigner le fruit de ses rêves. La méthode de travail mise en oeuvre à l'occasion de l'élaboration de ce disque est la résultante de lectures et recherches fournies de Barbara CARLOTTI au sujet des neurosciences, et en particulier des rêves, et d'une collaboration avec Perrine Ruby, docteure en neurosciences, chercheuse à l'Université de Lyon, au laboratoire Cortex (www.labex-cortex.com), dont les travaux sont principalement liés au sommeil, aux rêves et à la cognition.

[223] On parle depuis peu de neuro-architecture, discipline nouvelle ayant pour objet l'étude de l'influence des structures architecturales et des matériaux sur le cerveau. Il s'agit de dessiner les bâtiments de façon à ce que les individus qui y vivent ou travaillent n'éprouvent aucune sensation d'oppression, d'inconfort. Une Academy of Neurosciences For Architecture (anfarch.org) vient de voir le jour. Cf. À ce sujet, C. METZGER, Neuroarchitecture, Jovis 2018.

[224] Aux Etats-Unis, la discipline est bien plus assise ; on parle de Neurolaw. Les chercheurs sont nombreux à y consacrer des travaux et ouvrages. Voir notamment à ce sujet le site www.lawneuro.org de la MacArthur fondation research network on Law and Neurosciences, liée à l'Université Vanderbilt, de Nashville.

[225] On dénombre tout de même plusieurs publications, d'ailleurs bien référencées sur le site lawneuro.org http://www.lawneuro.org/france.php, mais néanmoins très peu nombreuses au regard de l'influence que les neurosciences pourraient exercer sur le droit.

[226] L'hypnose, à laquelle il s'était formé auprès de Bernheim, fut assez vite rejetée par Freud faute d'avoir pu l'expliquer scientifiquement ; elle est désormais couramment mise en oeuvre en médecine, notamment pour traiter la douleur ou anesthésier.

lors en tout cas que ces travaux contredisent la façon dont le droit les appréhende. Alors pourquoi cet hermétisme ? Peut-être faut-il y voir une nouvelle[227] illustration du penchant naturellement conservateur, rétif aux influences extérieures et à la transversalité de notre système juridique…

L'objet de cet article est par conséquent d'esquisser, de façon succincte mais, souhaitons-le, synthétique, la trame d'une typologie des interactions possibles entre les neurosciences cognitives et le droit, où seraient mises en lumière les améliorations que ce dernier pourrait en tirer. Une sorte de feuille de route de nouvelles explorations scientifiques. Rien ne dit que les bénéfices que peut en tirer le droit seront réels, mais la recherche mérite d'être conduite. Il s'agit donc d'un article introductif, d'une invite à une approche pluridisciplinaire et prospective.

Les neurosciences cognitives sont à même de faciliter l'accès au droit **(I)**, tant par le juriste que par le justiciable. Elles sont de nature à rendre la norme plus intelligible et mieux respectée. Les neurosciences peuvent également rendre la règle de droit plus adéquate au fonctionnement humain **(II)**, ce qui pourrait la rendre plus légitime et efficace.

On précise que les neurosciences sont très liées à un autre domaine de recherche actuel, l'intelligence artificielle, que ce soit par les moyens matériels que les neuroscientifiques emploient pour réaliser leurs travaux, que par les outils que lesdits travaux amènent à imaginer. On évoquera donc souvent l'intelligence artificielle, en tant que corollaire des neurosciences, dans cet article.

I) Le cerveau et l'accès au droit

Les principaux griefs que l'on adresse couramment au droit sont, d'une part, le foisonnement des normes, communément qualifié d'inflation législative et, d'autre part, l'imperfection de ces normes auxquelles il est reproché d'être

[227] Il suffit de voir avec quelle lenteur le droit s'adapte à la nouveauté. Les aspects juridiques de l'environnement numérique en fournissent de constantes illustrations ; un comportement litigieux, potentiellement illicite, disparaît souvent de a scène contentieuse avant même que le droit –qu'il s'agisse de la loi, du règlement ou de la jurisprudence- ne soit parvenu à le réguler harmonieusement, à l'appréhender.

confuses, incomplètes. Ce sont là deux aspects d'un même problème, celui de l'accès au droit, que l'on peut poser en ces termes : comment connaître, avec un degré de fiabilité suffisant, les droits et obligations d'une personne ? On peut raisonnablement croire que les progrès récents des neurosciences sont de nature à rendre le droit plus accessible, tant pour le professionnel dont la mission consiste précisément à éclairer des clients sur la licéité de leurs agissements **(A)** que pour le justiciable désireux de se conformer spontanément au droit **(B)**.

A) Le juriste

Grâce à l'internet, les règles de droit comme la jurisprudence n'ont jamais été aussi accessibles que depuis le début du XXIème siècle. Il n'a pourtant jamais semblé aussi difficile de saisir leur sens, leur contenu. Il s'agit probablement d'un effet pervers de leur abondance. Il suffit à cet égard de songer au nombre et à la longueur excessive des décisions de la Cour de justice et du Tribunal de l'Union européenne. Beaucoup d'étudiants et de praticiens le confessent : impossible de tout lire, de tout comprendre, bref de tenir ses connaissances à jour, même en cas d'exercice d'une activité spécialisée… Tant que la réduction du volume normatif restera un voeu pieu, pourquoi ne pas tirer profit des neurosciences pour faciliter l'accès au droit, non seulement durant la formation des juristes à l'Université **(1)** mais encore dans l'exercice de leur activité professionnelle **(2)** ?

1) L'apprentissage du droit par le juriste

Grâce aux technologies numériques, l'apprentissage du droit a considérablement évolué, dans le sens d'une plus grande rapidité d'accès à l'information et d'une optimisation du travail. Sans entrer dans les détails, il suffit à cet égard de rappeler le confort et le gain de temps liés au développement dans les universités des environnements numériques de travail (E.N.T.), des bibliothèques numériques, des abonnements à diverses bases de données et, dans une moindre mesure, de l'enseignement à distance, encore trop peu répandu.

Mais si les outils mis à la disposition des étudiants se sont renouvelés, les méthodes d'enseignement pratiquées en facultés de droit restent quant à elles très archaïques. A l'époque du podcast, du MOOC, du e-book, des serious games, quelques rares universitaires questionnent l'intérêt pédagogique de l'intouchable cours magistral et des centaines d'heures passées, chaque semestre, à prendre des notes sur la dictée d'un enseignant plus ou moins stimulant. A chaque correction de paquet de copies, à chaque session d'oraux, nous constatons que le volume des connaissances mémorisées par les étudiants est très inférieur à celui dispensé en cours et travaux dirigés. Cela pose au moins deux questions fondamentales quant à l'organisation des études de droit :

- la formation des juristes doit-elle toujours reposer sur l'exigence d'une mémorisation massive de connaissances, balayant toutes les branches du droit, au risque qu'en fin de cycle ou de parcours universitaire l'immense majorité de ces données ait fui la mémoire de l'apprenant ? La question est d'autant plus pertinente qu'en raison de l'impermanence de nombreuses normes, la quantité résiduelle de connaissances retenues sera partiellement obsolète lorsque l'étudiant sera devenu praticien.
- Le cours magistral prononcé en amphithéâtre doit-il rester l'alpha et l'oméga de l'enseignement de cette discipline ? Ne doit-on pas envisager d'en faire évoluer la forme ?
-

A chacune de ces questions, les neurosciences cognitives sont à même d'apporter des réponses novatrices.

S'agissant de la mémorisation, il serait temps de lui préférer le travail de la logique, du raisonnement, de la dialectique, vraisemblablement plus profitables à l'étudiant dans une structure professionnelle. Tous les outils numériques permettent de nos jours de trouver ou retrouver une donnée de fond en quelques secondes, dans une version de surcroît plus complète et à jour que celle que livrerait une mémoire humaine. Et si l'on estime l'apprentissage par coeur indissociable du droit, pourquoi alors ne pas enseigner à l'Université -voire bien avant- des méthodes permettant une mémorisation rapide et pérenne ? Et c'est là que l'on retrouve les neurosciences qui, à cet égard, ont permis de réaliser des progrès

spectaculaires. Cela suppose une petite révolution dans la structuration du planning hebdomadaire des étudiants en droit, qui devrait alors réserver une place bien plus grande à la méthodologie de l'apprentissage, et c'est, à cet égard, qu'une remise en cause du format du cours magistral pourrait précisément être opportune. Il ne serait pas absurde de conserver le cours magistral dans les matières fondamentales, comme celles à travaux dirigés, et lui trouver des substituts plus en accord avec les capacités effectives de mémorisation du cerveau pour les autres matières.

Le conservatisme du droit est d'autant plus incompréhensible que la plupart des spécialistes des sciences de l'éducation font, dans l'enseignement primaire comme secondaire, évoluer leurs pratiques pédagogiques à l'aune de ce que les neurosciences cognitives révèlent sur le fonctionnement cérébral, cela tant dans le sens d'un meilleur apprentissage que dans celui d'un accroissement du plaisir pris à travailler. L'actuel Ministre de l'Education, Jean-Michel Blanquer, a ainsi créé un Conseil scientifique pluridisciplinaire pour l'école, présidé par Stanislas Dehaene, neuroscientifique, psychologue cognitiviste et professeur au Collège de France, chargé entre autres missions de traduire en propositions le fruit de ces découvertes. On regrette que les Facultés de droit n'aient pas encore songé au profit qu'elles pourraient en tirer.

2) La pratique du droit par le juriste

A ce sujet, le droit a déjà amorcé sa révolution. La simplification du travail est à l'oeuvre pour ceux des praticiens qui recourent à ce que l'on appelle les Legaltechs ou encore outils de justice prédictive. Il s'agit en quelques sortes d'instruments numériques chargés d'effectuer le travail d'identification exhaustive et de synthèse des informations juridiques nécessaires à la résolution d'un problème de droit, afin d'épargner au juriste un travail de recherche fastidieux, chronophage et surtout insécure compte-tenu de la pléthore de sources pertinentes. Les Legaltechs se développent considérablement depuis quelques mois et beaucoup les présentent comme l'avenir de la pratique du droit.

On pourrait s'interroger sur le rapport entre ces outils d'intelligence artificielle et ce que les neurosciences apprennent du fonctionnement du système cérébral. Le lien existe, mais n'est pas apparent à première vue, dans la mesure où, dans l'usage des legaltechs, les enseignements des neurosciences cognitives ne doivent pas être mis en oeuvre par le juriste lui-même, mais plutôt par les ingénieurs qui élaborent ces outils de justice prédictive. Ceux-ci doivent, en effet, veiller à ce que le travail de sélection des données soit qualitativement et quantitativement aussi -voire plus- juste et fouillé que celui qu'effectuerait un individu au meilleur de ses aptitudes intellectuelles. Le fonctionnement de l'outil doit donc *a priori* s'inspirer de celui du cerveau pour mener à des raisonnements juridiques fiables. Ici, les neurosciences interviennent préalablement au travail du juriste afin d'alléger et de simplifier l'accomplissement de sa mission.

Les legaltechs sont très décriées. On leur reproche en substance de mécaniser le travail du juriste et de lui faire perdre une grande part de son libre arbitre. Il est pourtant possible d'envisager le point de vue inverse. On peut effectivement soutenir que le tri des informations de fond pertinentes est intellectuellement ingrat -ne s'en déleste-t-on pas couramment, dans les cabinets, sur des stagiaires ?- et que l'essence du travail du juriste réside dans la façon de sélectionner les données qu'il exploitera et de les articuler dans un raisonnement structuré, clair et convaincant ? Aussi paradoxal que cela puisse paraître, des outils de legaltech performants, s'ils sont paramétrés conformément aux schèmes de l'esprit humain, doivent permettre au praticien de faire l'économie d'efforts de mémorisation et de recherches de nos jours devenus injustifiés[228], et de retrouver le temps et la disponibilité d'esprit nécessaires à l'imagination, la maturation d'une démonstration juridique. Or là réside sans doute l'aspect intellectuellement le plus attractif du travail du juriste… Loin de conduire à un remplacement du praticien du droit par la machine, les legaltechs devraient lui fournir l'occasion de se focaliser sur la partie la plus subjective, donc la plus humaine et, en l'état actuel de la science, inexécutable par un algorithme, de son ouvrage. Une forme de retour à l'essentiel, à l'artisanat… En d'autres termes, une libération plus qu'un asservissement.

[228] Cf. ce que l'on a exprimé en 1 au sujet de la formation des juristes.

Mais les neurosciences pourraient en outre faciliter l'accès au droit des non juristes.

B) Le sujet de droit

L'adage « Nul n'est censé ignorer la loi » constitue la clef de voûte de notre système juridique ; il conditionne l'opposabilité de la règle de droit aux justiciables. Peut-on s'en satisfaire quand juristes comme sujets de droit s'accordent à admettre que les règles de droit sont trop nombreuses et parfois confuses ?

Internet et l'intelligence artificielle ont sensiblement facilité l'accès du justiciable à la règle de droit. Diverses bases de données en ligne lui offrent de trouver et lire toute norme en vigueur, nationale comme européenne, ainsi que de nombreuses décisions de justice[229]. Il n'est plus nécessaire de s'aventurer dans la consultation de journaux officiels « papier » ou de revues de jurisprudence dont le maniement est quasiment impossible à des non avertis. Pour le sujet de droit qui ignore le texte de référence, il existe également des bases de données permettant, à partir de mots clefs, de lister les textes ou dispositions liés -de façon plus ou moins directe- à une question de droit donnée, comme par exemple le site service-public.fr. Cela étant, ces outils ne sont pas toujours exploitables par des non-juristes quand la qualification de la question de droit ne correspond pas à un mot ou une locution issu du langage courant (« problème de voisinage », par exemple) mais suppose une certaine maîtrise du jargon (« forclusion par tolérance », par exemple). Un système d'intelligence artificielle pourrait néanmoins, pas à pas, par une série plus ou moins longue d'interrogations de l'usager, parvenir à qualifier son problème de droit et à lui fournir la liste des textes applicables.

Mais l'accès automatisé à la règle en vigueur ne rend pas pour autant sa compréhension et son application, au cas d'espèce, aisées pour le sujet de droit. Or, nombre d'entre eux, par négligence ou manque de moyens, ne font

[229] Les sites d'information juridique sont très nombreux, mais il n'est pas certain qu'ils permettent une meilleure connaissance du droit, car il n'est aisé de distinguer les contenus exacts et à jour des publications erronées.

pas la démarche, en cas de doute, d'aller consulter un professionnel du droit. A cet égard, neurosciences et intelligence artificielle pourraient s'avérer très prometteuses.

Une première solution consisterait à créer des outils de Legaltech destinés aux justiciables, qu'on pourrait nommer outils de justice préventive. Ces outils agrègeraient les normes textuelles aux interprétations et précisions que la jurisprudence leur apporte, de façon à avoir un état aussi détaillé que possible du droit. Ils pourraient ensuite offrir au justiciable, par un enchaînement arborescent de questions, de cerner son problème de droit, et d'y apporter une solution ou, à tout le moins, de lui indiquer les solutions susceptibles d'y être appliquées avec leur degré de probabilité. Les neurosciences doivent avoir une place importante dans l'élaboration de ce type d'outils, car le cheminement des questions posées au client doit non seulement être logique, mais apte à identifier sa manière de raisonner, et en particulier les éventuelles ellipses qu'il aurait inconsciemment commises dans la relation des faits ou dans l'exposé de ses prétentions. Ces nouveaux outils, pour l'instant expérimentaux, devraient non seulement permettre de rendre le droit accessible à des individus qui n'iraient jamais consulter un avocat -pour raisons financières par exemple- mais encore de prévenir l'apparition de litiges courants, facilement évitables, ce qui libèrera les praticiens, et spécialement les magistrats, de ces contentieux encombrants et chronophages. Doit-on craindre qu'une démocratisation des legaltechs destinées aux sujets de droit menace l'activité des professionnels du droit ? On ne le pense pas, car les litiges subtils nécessiteront, longtemps encore, des raisonnements humains. Les legaltechs doivent plutôt être envisagées comme des instruments de filtrage, d'écrémage des affaires basiques. En outre, la création et la mise à jour constante des outils de legaltech supposeront une importante main d'oeuvre de professionnels du droit.

Une autre voie, plus futuriste mais réaliste, pourrait consister à conjuguer intelligence artificielle et neurosciences afin de simplifier la législation. On peut, tout d'abord, imaginer que le travail d'identification des textes obsolètes ou inappliqués soit robotisé, en particulier à partir d'une observation de leur fréquence dans la jurisprudence. Il ne resterait plus alors au législateur qu'à

vérifier la pertinence de cet état des lieux et de procéder à une abrogation effective desdites normes. On pourrait également envisager que la rédaction ou, à tout le moins, la vérification de la rigueur sémantique et logique des textes, soit assistée par un système d'intelligence artificielle. Les textes actuels abondent d'imprécisions, d'erreurs, d'oublis, d'absence de définitions des notions, de contradictions. Ils ne sont souvent pas intrinsèquement compréhensibles, même de professionnels du droit ; la mise en oeuvre d'une disposition nouvelle est par conséquent fréquemment suspendue à l'élaboration, lente par hypothèse, d'une interprétation jurisprudentielle uniforme. Il n'est pas farfelu d'imaginer qu'un robot puisse traquer ces défauts et inviter le législateur à les corriger avant l'adoption du texte ; l'objectif étant d'aboutir à la rédaction de textes normatifs aisément compréhensibles de tous, et particulièrement des justiciables qui en sont destinataires, pour ce qui est de leurs règles essentielles. L'intelligence artificielle est en effet capable de produire des contenus qui jusque alors étaient l'apanage de l'intelligence humaine. Certaines machines savent par exemple composer des partitions musicales à la manière de tel ou tel compositeur. Ross Goodwin, artiste, hacker et codeur américain, a récemment publié un livre intitulé « 1 the road », entièrement écrit par un système d'intelligence artificielle qu'il a lui-même créé. Ce livre retrace un « road trip gonzo », sur le modèle des oeuvres de Jack Kerouac. De plus en plus d'éditeurs de presse recourent à l'écriture d'articles par des robots ; c'est le cas par exemple du Washington Post[230] ou du New York Times[231] ; il ne s'agit pas pour l'heure d'articles de fond, mais plutôt de news ou d'articles retraçant le déroulement d'une épreuve sportive. Certains programmes dépassent même l'humain dans des tests de compréhension de lecture ou dans des jeux de logique comme les échecs ou le Go. Grâce au machine Learning, l'intelligence artificielle devrait être en mesure d'apprécier la lisibilité ou la rigueur syntaxique et la logique d'un texte de loi élaboré par l'humain de façon à traquer ses imperfections[232]. Un paramétrage lié aux destinataires du texte devrait permettre d'adapter son degré d'intelligibilité au public visé ; une loi de droit commercial applicable à des professionnels

[230] Voir son système d'AI nommé Heliograf.

[231] Et de son système Editor.

[232] Il n'est même pas exclu d'imaginer qu'une machine soit capable de le rédiger seule ; Cela aboutirait vraisemblablement à des lois d'un style littéraire très nouveau, mais si elles sont mieux comprises et respectées…

compétents ne serait pas jaugée de la même façon qu'une loi de droit civil relative à tout individu. Il ne faut pas considérer ces supputations comme une rêverie fantaisiste d'amateur de science-fiction. Les progrès en ces domaines sont si surprenants que certains esprits vont jusqu'à envisager la possibilité prochaine d'une intelligence artificielle tenant les rênes d'un Etat[233]. Son acceptation par la communauté juridique et politique et son usage risquent d'être davantage problématiques…

II) Le cerveau et l'adéquation du droit

La crise de légitimité que connaît le droit tient non seulement à la complexité du système judiciaire et à l'inflation des normes, mais également à l'inadéquation de certaines règles au fonctionnement du cerveau humain. Les neurosciences cognitives sont porteuses de nombreux enseignements sur la façon dont le cerveau et le système nerveux travaillent, qui permettent d'expliquer scientifiquement certains agissements jusqu'alors exclusivement imputés à l'exercice, défaillant ou bien conforme aux intérêts sociaux, d'un libre arbitre. En tenir compte dans le cadre de la rédaction d'une norme, qu'elle soit de fond **(A)**, de preuve ou qu'elle édicte une sanction **(B)**, pourrait être de nature à rendre le droit mieux accepté, plus efficace.

A) Le fond du droit

Bien qu'il semble logique de considérer le droit et la psychologie comme deux sciences humaines étroitement liées, leurs interactions sont en pratique assez rares. Leurs relations sont certes étudiées par la doctrine[234], mais de façon très marginale. En outre, jamais, dans un cursus de droit, on n'entend parler explicitement de la psychologie et de son influence sur l'élaboration ou l'application de la norme, sur l'appréhension et la qualification juridique d'un comportement humain. Plusieurs raisons sont à l'origine de cette distance. Une première tient au fait que le droit, et notamment le droit objectif, doit être défini de façon abstraite, indépendante des vicissitudes de la psyché ; la règle

[233] https://www.huffingtonpost.fr/2019/03/21/une-intelligence-artificielle-au-pouvoir-1-francais-sur-4-serait-daccord_a_23697549/

[234] Voir par exemple les travaux de la Société Française de Psychologie Juridique (SFPJ): https://psycho-droit.com .

de droit doit être identique pour tous les justiciables, et par conséquent, rédigée en songeant à un personnage de référence standard : le consommateur moyen, le bon père de famille etc… Une fois entrée en vigueur, certains individus s'avèreront plus respectueux de la norme que le standard et d'autres moins, voire pas du tout. Mais on peut aussi expliquer l'indifférence du droit pour la chose psychologique par le fait que l'interprétation des comportements humains et les moyens de réguler ou corriger ceux qui semblent contraires aux intérêts sociaux, ont longtemps été perçus comme très subjectifs, susceptibles de varier d'un spécialiste de la psychologie à l'autre et, en particulier, d'une école doctrinale à l'autre. Il suffit à ce sujet de songer à l'opposition assez radicale entre ses deux principaux courants contemporains que sont la psychanalyse et les thérapies cognitivo-comportementales. Cela étant, cet argument est très discutable dans la mesure où le droit est lui aussi très subjectif dans sa façon d'appréhender les comportements humains : les querelles doctrinales empreintes de préjugés moraux, éthiques, religieux, politiques dominent encore très largement la régulation juridique de la vie en société. Les divergences relatives à des sujets aussi sensibles que l'égalité des sexes, la soumission à l'impôt, le transsexualisme en sont de bonnes illustrations… Les neurosciences pourraient sur ce plan faire changer la perception que les juristes ont de l'influence de la psychologie sur le droit chaque fois qu'elles offrent une interprétation scientifique intangible à certains comportements. L'encadrement et la régulation juridique du comportement ne seraient plus parasités par la prise en compte de considérations subjectives mais exclusivement guidées par la réalité scientifique de l'humain. L'adéquation de la règle de droit au fonctionnement du cerveau la rendrait probablement plus légitime et plus facilement applicable, voire plus naturellement appliquée. L'influence des neurosciences sur la définition du licite pose non seulement la question de savoir s'il doit être apprécié au regard de ce qu'un humain ou son cerveau est capable de faire ou au regard des troubles qu'il cause à la société, quelles que soient ses capacités à juger de ses faits ou actes ; mais elle interroge encore sur la capacité de la loi à contredire, au nom d'intérêts subjectifs et partisans, les principes scientifiques, physiologiques de fonctionnement du cerveau.

La proposition de loi sur l'interdiction de la fessée et des violences éducatives, déposée par la députée MODEM Maud Petit, et adoptée à l'Assemblée nationale en novembre, et celle déposée au Sénat par l'ex-ministre socialiste Laurence Rossignol, et adoptée en mars, en fournissent une très bonne illustration. Elles visent à interdire le droit de correction dans les familles -fessée, gifle, tape etc.- qui, bien que toute maltraitante physique sur un enfant soit prohibée par le Code pénal, est toléré par une jurisprudence datant du XIXème siècle. L'objet de ces dispositions n'est pas partisan : elles ne cherchent pas à imposer aux familles de pratiquer ce qu'il est usuel de nommer la parentalité bienveillante au détriment d'une forme autoritaire, plus classique, d'éducation. De nombreux psychologues conseillent d'ailleurs une attitude de juste milieu[235], majoritairement bienveillante, mais fondamentalement ancrée sur certaines exigences incontournables que l'enfant doit observer, sans pour autant que leur méconnaissance soit sanctionnée par des sévices physiques. Ces propositions de lois s'inspirent des enseignements des neurosciences, notamment démocratisés par la pédiatre Catherine Gueguen[236], qui démontrent que les violences éducatives ordinaires peuvent avoir un effet délétère sur le développement du cerveau de l'enfant et se traduire, en particulier à l'adolescence, par anxiété, dépression, addictions. Les tenants d'une éducation plus ferme ne sont donc pas stigmatisés et, contrairement à ce que certains députés ou sénateurs représentant d'une tradition éducative sévère ont prétendu à l'occasion des débats, il ne s'en suivra aucune ingérence dans la vie des familles.

L'exemple des violences éducatives ordinaires est d'actualité, mais il peut sembler limité. Il n'est pas question dans cet article d'établir une typologie des branches ou des questions de droit dans lesquelles les neurosciences cognitives pourraient conduire à une redéfinition rationnelle et efficiente des normes ; elles sont assurément nombreuses. Il s'agit d'un sujet vaste.

B) La preuve et la réparation

[235] V. Par exemple Anne BACUS, L'autorité, pourquoi, comment : Pourquoi est-il nécessaire de poser des limites à nos enfants ?, Marabout 2014.

[236] V. par exemple, Pour une enfance heureuse: repenser l'éducation à la lumière des dernières découvertes sur le cerveau, Robert Laffont 2014.

C'est peut-être en matière de preuve et de réparation que les neurosciences cognitives associées à l'intelligence artificielle sont à même de révolutionner le monde du droit.

Les neurosciences ont été stimulées par les progrès remarquables réalisés en matière d'imagerie cérébrale. Un nouveau type d'IRM notamment, l'IRM fonctionnelle, visualise le cerveau en action et révèle comment fonctionnent ses différentes zones, ce qu'elles commandent.

La neuroimagerie moderne a ainsi permis de mettre en évidence que les zones cérébrales activées ne sont pas les mêmes en cas de mensonge ou de vérité. Grâce à cette découverte, on peut savoir si un individu dit la vérité ou ment avec un taux d'exactitude supérieur à 90%. On peut savoir si un individu en reconnaît un autre, s'il a déjà fréquenté un lieu etc. On saisit donc immédiatement l'impact d'une telle innovation en droit de la preuve, et pas seulement en matière pénale. Les rapports entre la vérité et le droit pourraient s'en trouver bouleversés.

Par ailleurs, de très nombreux travaux scientifiques sont consacrés aux mécanismes cérébraux à l'oeuvre dans le processus de décision[237]. Les neurosciences pourraient par conséquent permettre de savoir si un individu a agi intentionnellement ou non, s'il a réellement consenti à un acte juridique ou s'il y a consenti sans avoir une connaissance réelle de la portée juridique de son engagement. La preuve de conditions aussi fondamentales que le consentement, son intégrité, ses vices, en droit civil -obligations, mineurs et majeurs protégés- en droit de la consommation, cesserait d'être problématique. Rappelons qu'on sait depuis peu que l'âge de la maturité cérébrale est scientifiquement situé autour de vingt-cinq ans, alors que celui de la majorité légale est de dix-huit ans.

Les outils permettant de réaliser ces mesures sont pour l'instant très expérimentaux, mais il n'est pas farfelu d'imaginer qu'ils deviennent rapidement des accessoires du quotidien. Au temps où des montres

[237] V. Les travaux du Professeur de neurologie P. DAMIER, *Décider en toute connaissance de soi : Neurosciences et décision*, Odile Jacob 2014.

connectées effectuent des électrocardiogrammes sans même que l'usager ne s'en aperçoive, rien n'interdit de penser que, dans un avenir proche, il soit possible de savoir, par un dispositif technologique relié à un appareil connecté comme un smartphone, si le clic ou le toucher qu'un individu appose sur cet outil pour acheter ou louer un bien, un service, ou réaliser tout autre acte juridique est impulsif ou intentionnel. Ou encore de savoir si les clauses d'un contrat qu'il est nécessaire d'avoir lues avant de s'engager ont effectivement été compulsées.

Il reste à envisager le rôle des neurosciences dans la détermination d'une sanction. L'efficacité des sanctions, et en particulier de l'emprisonnement, est au coeur du débat social depuis de nombreuses années. Des expérimentations alternatives sont conduites : bracelet électronique, prisons ouvertes, TIG. Certaines sont efficaces sur certains sujets, d'autres moins. Il n'est pas exclu que les neurosciences soient en mesure de jauger avec un certain degré de fiabilité quelle sanction est la plus adaptée à un individu donné, en ce qu'elle est la plus à même d'encourager sa réinsertion ou en ce qu'elle réduit son risque de récidive. Cette démarche, à la supposer possible et fiable, ne pourrait bien sûr être mise en oeuvre qu'avec l'accord de l'auteur de l'infraction, mais s'il s'y soumet, on peut imaginer qu'il en résulterait une réduction très nette du nombre de personnes emprisonnées. L'enjeu social comme économique est donc important.

Ces réflexions, répétons-le, ne sont que des supputations relatives à ce que les neurosciences pourraient apporter au monde du droit dans un avenir plus ou moins proche. Elles ne doivent pas être considérées comme irréalistes ou probables, mais plutôt comme des objets d'études ou de travaux qu'il serait bon de confier conjointement à des juristes et des neuroscientifiques. Il n'est pas question de prétendre que tout est neuronal ; certains scientifiques « neurosceptiques » s'insurgent d'ailleurs à ce propos, tout comme d'autres il y a quelques années au sujet du tout génétique. La conclusion est ailleurs : il s'agit de souligner qu'il est temps que l'indifférence des juristes à l'égard des neurosciences cesse.

Prédiction et décision, l'exemple de la médecine

Paul VÉRON

Maître de conférences à l'université de Nantes
Laboratoire Droit et Changement Social (UMR CNRS 6297)
Chercheur associé au CERDACC

La médecine est dite prédictive lorsque les actes qu'elle met en œuvre n'ont pas pour but de diagnostiquer une pathologie actuelle mais les risques de développement futur d'une pathologie chez un ou plusieurs individus, avant l'apparition de symptômes[238].

Elle se situe donc davantage du côté du pronostic (ce qui sera) que du diagnostic (ce qui est). Toutefois, comme ce dernier, elle relève du champ de la connaissance et non de l'action. Prédire n'est pas prévenir. Annoncer ce qui sera demain n'est pas la même chose que mettre en œuvre les moyens propres à l'empêcher. Les deux démarches sont malgré tout le plus souvent liées. En effet, de même que le diagnostic d'une maladie présente va constituer une étape essentielle dans la détermination et la mise en œuvre du traitement curatif, les données prédictives pourront conduire à la mise en œuvre de traitements préventifs ou plus largement d'actions de prévention.

La généralisation de l'expression « médecine prédictive » est relativement récente et date du milieu des années 1990[239]. Elle correspond peu ou prou au développement de la médecine du génome et l'identification de l'origine génétique -partielle ou totale – de certaines maladies ainsi que des prédispositions génétiques à leur développement.

Pour autant, la démarche de prédiction est aussi ancienne que la médecine elle-même. Le médecin qui établit son pronostic sur l'évolution de la maladie du patient formule une prédiction. Il en va de même lorsqu'il évalue le

[238] V., M.-F. CALLU, G. ROUSSET, M. GIRER, *Dictionnaire de droit de la santé*, LGDJ, 2017, « Médecine prédictive » ; A. BOUÉ, *Qu'est-ce que la médecine prédictive ?*, *in* Les lois bioéthiques à l'épreuve des faits, PUF, 1999, p. 165.

[239] On attribue l'expression au professeur Jacques RUFFIÉ, *Naissance de la médecine prédictive*, Odile Jacob, 1993.

pourcentage de risques de complications impliquées par un traitement ou une intervention chirurgicale[240]. Enfin, le diagnostic d'une hypertension, d'un diabète ou d'une hypercholestérolémie chez un sujet permettent de prédire un risque, à moyen ou long terme, de complications cardiaques ou d'accident vasculaire cérébral. Et que dire de la vaccination, démarche de prévention, qui s'appuie sur des prévisions[241] quant aux risques de développement de certaines maladies au sein de la population, en particulier les risques d'épidémies ?

La prédiction n'est donc pas propre à l'étude des caractéristiques génétiques de l'être humain[242]. Malgré tout, le développement contemporain de la génétique permet d'envisager une extension importante du champ de la médecine de prédiction[243]. Le séquençage du génome humain permet d'ores et déjà d'identifier les prédispositions génétiques à un ensemble de pathologies. Il s'agit en d'autres termes d'associer la présence d'une anomalie ou mutation génétique à l'apparition ou au risque d'apparition d'une affection déterminée.

On pressent qu'il y a là des enjeux éthiques[244] et financiers considérables, avec notamment le développement d'un marché des tests génétiques[245], mais

[240] L'article L. 1111-2 du code de la santé publique dispose en ce sens que le médecin doit notamment informer le patient *« des risques fréquents ou graves normalement prévisibles »* associés aux actes d'investigation ou de traitement, mais aussi des *« conséquences prévisibles en cas de refus »* exprimé par le patient.

[241] La distinction entre prédiction et prévision n'est pas évidente. Au sens littéral, la prédiction implique une annonce (pré*dire*) que n'implique pas la prévision (pré*voir*). Elle semble entretenir un lien étroit avec l'idée de message ou d'information délivrée à un ou des tiers. En outre, le terme « prédiction » peut être utilisé pour caractériser des situations où il existe une incertitude sur la réalisation d'un évènement futur, pour ce qui nous concerne, la déclaration d'une maladie. La prévision désignerait au contraire les situations où il existe davantage de certitudes. La prédiction a d'ailleurs une connotation plus mystique, que n'a pas la prévision. L'expression « médecine prédictive » suggérerait-elle que la capacité à modéliser le devenir de la santé d'un patient constitue fondamentalement une science inexacte ?

[242] P. PUJOL, *Médecine prédictive*, in Médecine, maladie, société. L'éthique médicale, Sauramps médical, 2008, p. 115 : *« Au sens large, le champ de la médecine prédictive ne se limite pas à celui des prédispositions aux maladies génétiques. Il comprend également celui d'affections très courantes, au premier rang desquelles les maladies cardiovasculaires dont les marqueurs sont le diabète, l'hypercholestérolémie et l'hypertension artérielle. Ainsi, le diagnostic de diabète, c'est-à-dire d'un défaut de régulation des sucres aboutissant à une hyperglycémie (présence d'un taux élevé de sucre dans le sang), est plutôt le diagnostic d'un symptôme que d'une maladie. Mais celui-ci est un facteur prédictif d'un risque important de complication vasculaire, notamment ».*

[243] V., CCNE, avis n° 46, Génétique et médecine : de la prédiction à la prévention, 30 oct. 1995 ; I. VACARIE, « Examens génétiques et médecine prédictive », *RDSS* 1993, p. 429.

[244] Sur les dangers du « tout génétique » : J. GAYON, « Prédire ou expliquer ? » Sciences et avenir, Hors-série, « L'Empire des gènes », oct. Nov. 2003 ; G.-E. SERANILI, *Génétiquement incorrect*, Paris, Flammarion, 2003 ; F. RAMUS, « Quel pouvoir prédictif de la génétique et des neurosciences, et quels problèmes ? », Médecine et droit 2011, n° 106, p. 51.

[245] V. not. les actes du colloque « Accès aux tests génétiques en Europe », *RGDM*, n° 42, mars 2012.

aussi des traitements et actions visant à prévenir l'apparition des pathologies prédites. Il n'est pas étonnant, dès lors, que cette médecine de prédiction, en particulier l'étude des caractéristiques génétiques, fasse l'objet d'un encadrement par la loi et suscite d'importants débats[246].

Deux ordres de difficultés peuvent être identifiés en ce qui concerne la prédiction en médecine. Premièrement, jusqu'où faut-il prédire ? A quelles conditions la démarche de prédiction apparaît-elle éthiquement légitime et juridiquement fondée ? La recherche des prédispositions pathologiques d'un individu est le résultat d'une décision qui ne va pas de soi et n'est pas sans conséquences pour la personne concernée et plus largement pour la société. Il importe dès lors de s'intéresser aux critères qui justifient une telle démarche. Deuxièmement, que faire de la prédiction une fois établie ? C'est la question des suites à donner aux résultats prédictifs, qui se pose au moins à deux niveaux : celui de l'information qui doit être délivrée, mais également celui des éventuelles actions de préventions qui peuvent être entreprises. Il importe ainsi de se pencher à la fois sur les conditions (**I**) et les conséquences de la prédiction (**II**), c'est-à-dire tant sur la décision prédictive elle-même que sur les décisions qui pourront en découler.

I) Les conditions de la prédiction

L'encadrement de la décision prédictive porte tant sur les modalités (A) que sur les finalités de celle-ci (B).

A) Le contrôle des modalités

L'auteur. Le droit médical organise un monopole du médecin, et par exception d'autres professions de santé, sur tout acte de diagnostic ou de traitement, à travers l'incrimination d'exercice illégal de la médecine[247]. Selon un critère jurisprudentiel bien établi, ces actes sont définis au regard de leur finalité[248]. Toute démarche visant à identifier la nature d'une pathologie ou à

[246] C. DABURON, « Médecine prédictive : les dangers d'un nouveau pouvoir », *RDSS* 2001, p. 453.
[247] CSP, art. L. 4161-1.
[248] Not., C. COUSIN, « Vers une redéfinition de l'acte médical », *RGDM*, 2017, n° 63, p. 93.

proposer des remèdes pour la traiter ne peut être accomplie que par un médecin, sauf à s'exposer à une sanction pénale[249]. La décision prédictive n'échappe pas à ce régime dès lors qu'elle vise à prédire l'évolution de l'état de santé de l'individu et en particulier l'avènement futur, certain ou probable, d'une pathologie déterminée.

Par conséquent, et quand bien même ce diagnostic ne supposerait pas d'acte invasif, il ne peut être pratiqué par une personne n'étant pas juridiquement habilitée. S'agissant de l'examen des caractéristiques génétiques, la loi est encore plus stricte. L'examen ne peut être pratiqué que sur prescription médicale[250] par des « praticiens agréés »[251] par l'Agence de biomédecine ou sous leur responsabilité. Ces praticiens peuvent au demeurant être médecin ou pharmacien et doivent, pour l'obtention de l'agrément, justifier d'une formation spécialisée et d'une expérience professionnelle jugées suffisantes, pour la catégorie d'analyses concernée (cytogénétique, génétique moléculaire, ou autres analyses de biologie médicale)[252]. De même, les laboratoires de génétique humaine doivent être accrédités.

Bien qu'aucun texte ne le prévoie de manière explicite, il résulte de ce cadre juridique l'interdiction pour des acteurs privés de commercialiser des tests génétiques à destination du public, aussi appelés tests génétiques en accès libre (TGAL)[253]. La régulation de la commercialisation de ces tests est toutefois délicate dès lors que d'autres pays ne l'interdisent pas et que leur vente par des entreprises étrangères se fait le plus souvent à distance par internet. *« Cette offre est réalisée par des entreprises majoritairement situées aux Etats-Unis qui proposent, à partir d'un auto-prélèvement de salive, de délivrer directement aux individus des informations sur leur santé (diagnostic de maladies monogéniques ou pourcentage de risques de développer une maladie multifactorielle) »*[254].

[249] V., P. MISTRETTA, *Droit pénal médical*, Cujas, 2013.
[250] CSP, art. R. 1131-4 et s.
[251] CSP, art. L. 1131-3
[252] CSP, art. R. 1131-7.
[253] V. ANASTRAZOVA, E. RIAL-SEBBAG, « Les tests génétiques en accès libre accès : quelle protection pour le consommateur européen », *RDSS* 2012, p. 817. E. SUPIOT, « Consommateur de tests génétiques, un patient avisé ou berné », *RDC* 2009, p. 1573.
[254] E. RIAL-SEBBAG, **«** Protection juridique des usagers de tests génétiques en accès libre, une protection nécessaire ? », *RGDM*, 2012, n° 42, p. 29.

Curieusement, le législateur a prévu une sanction pénale non seulement pour les personnes – physiques ou morales – qui commercialiseraient mais également pour les consommateurs, ce qui apparaît plus contestable[255]. Il est vrai que les informations génétiques résultant d'un dépistage pouvant avoir un impact non seulement sur la personne mais également son entourage, elles ne touchent pas uniquement à la liberté individuelle de l'intéressé. La fiabilité, tant des conditions de réalisation que des résultats de ces tests ne pouvant être contrôlée[256], le législateur a jugé nécessaire de dissuader fermement les individus d'y recourir. L'article 226-28-1 du Code pénal créé par la loi du 7 juillet 2011[257] sanctionne ainsi de 3750 euros d'amende *« le fait, pour une personne, de solliciter l'examen de ses caractéristiques génétiques ou de celles d'un tiers ou l'identification d'une personne par ses empreintes génétiques en dehors des conditions prévues par la loi »*. Jusqu'à l'adoption de ce texte, seuls les tiers pouvaient être poursuivis.

Le processus. Comme tout acte médical, le diagnostic prédictif est soumis à un certain nombre de conditions préalables, à commencer par le consentement éclairé de son destinataire. *« Aucun acte médical ni aucun traitement ne peut être pratiqué sans le consentement libre et éclairé de la personne et ce consentement peut être retiré à tout moment »*[258]*.* En matière d'examen des caractéristiques génétiques, les conditions sont là encore plus strictes puisque le consentement de la personne *« doit être recueilli par écrit préalablement à la réalisation de l'examen, après qu'elle a été dûment informée de sa nature et de sa finalité »*[259], consentement révocable sans forme et à tout moment, tandis que le Code pénal assortit la violation de cette règle d'une peine d'emprisonnement et d'amende[260].

Plus délicate est la question de l'information préalable à l'examen. Le contenu de cette information est précisé par l'article R. 1131-4 du Code de la

[255] *Ibid.*

[256] CCNE, avis n° 105, Questionnements pour les Etats généraux de la bioéthique, 9 oct. 2008, p. 6 : *« la diffusion incontrôlée par internet de tests génétiques (…) constitue un moyen de contourner la loi française. En outre, l'information des personnes qui y ont recours n'est pas assurée de façon satisfaisante, ni avant les tests, ni concernant leurs résultats ».*

[257] Loi n° 2011-814 du 7 juillet 2011 relative à la bioéthique ; J.-R. BINET, « La réforme de la loi bioéthique. Commentaire et analyse de la loi du 7 juillet 2011 », LexisNexis Actualité, 2012, p. 6, n° 17.

[258] CSP., art. L. 1111-4 al. 4.

[259] C. civ., art. 16-10.

[260] C. pén., art. 226-25.

santé publique : *« Préalablement à l'expression écrite de son consentement, la personne est informée des caractéristiques de la maladie recherchée, des moyens de la détecter, du degré de fiabilité des analyses ainsi que des possibilités de prévention et de traitement. En outre, elle est informée des modalités de transmission génétique de la maladie recherchée et de leurs possibles conséquences chez d'autres membres de sa famille »*.

La délivrance de l'information en génétique pose des difficultés à l'heure où il est devenu techniquement possible, et économiquement soutenable, d'envisager un examen de l'entier génome de l'individu. Le traitement des données secondaires constitue sur ce point un problème majeur. Une donnée secondaire est une donnée recherchée pendant l'examen génétique mais sans lien avec la donnée primaire, c'est-à-dire la raison de l'examen génétique. En pratique, le recours à une analyse génétique sera justifié par l'existence chez le sujet d'une pathologie ou d'un handicap dont on souhaite identifier l'origine, ou encore par la présence d'une anomalie génétique chez un membre de la famille. Dans ce cas, la recherche est dite « ciblée », parce qu'orientée sur une anomalie déterminée. Or, les progrès de la génétique permettent aujourd'hui d'identifier de très nombreuses pathologies associées à des anomalies d'un gène. Dans ce contexte, les recommandations de plusieurs sociétés savantes préconisent d'étendre systématiquement, lorsqu'un examen est réalisé, le champ de la recherche à d'autres anomalies génétiques éventuelles, et ainsi de recueillir des « données secondaires ». A titre d'exemple, l'*American College of Medical Genetics and Genomics (ACMG)* a publié une liste de 59 anomalies génétiques qu'elle préconise de rechercher activement lors de chaque séquençage de l'exome ou du génome d'une personne[261].

La question de l'information sur les données secondaire en génétique pose un problème propre à la médecine prédictive puisqu'il s'agit d'informer non pas sur les caractéristiques d'une pathologie actuelle mais sur un ensemble d'anomalies éventuelles et les pathologies qui leurs sont associées[262]. Or, ces

[261] S. KALIA, K. ADELMAN, S. BALE, *et al,* Recommendations for reporting of secondary findings in clinical exome and genome sequencing, 2016 update : a policy statement of the American College of Medical Genetics and Genomics, *in Genetics in Medicine*, vol 19, n°2, feb. 2017, p249, cité par M. GUILLET, *La question des données secondaires en génétique. Réflexion éthique et philosophique*, Mémoire de Master, Université de Nantes, 2018.

[262] Une interrogation similaire peut avoir lieu à propos de l'information sur les risques d'une intervention chirurgicale ou d'un médicament, information sur des événements dont la réalisation future est incertaine.

anomalies peuvent avoir une portée extrêmement diverse selon qu'elles concernent des pathologies monogéniques ou multifactorielles, selon les caractéristiques du patient, son environnement familial, ses habitudes de vie, mais aussi selon le degré de certitude scientifique concernant l'association entre l'anomalie et la prédisposition pathologique considérée. La délivrance d'une information *« claire, loyale et appropriée »*[263] sur l'ensemble des éléments exigés par la loi semble délicate dans ce contexte lorsqu'on sait qu'une consultation génétique préalable à l'examen dure environ 45 minutes dont maximum 15 minutes sont consacrées à l'information du patient[264]. La généralisation de la recherche de données génétiques secondaires – déjà pratiquée en France par certains laboratoires - n'est ainsi pas sans incidences sur les difficultés à recueillir un consentement éclairé. Le changement d'échelle affecte le processus de décision.

B) Le contrôle de finalités

Le but. De même que toute atteinte au corps doit être justifiée par une nécessité médicale, la loi dispose que « *l'examen des caractéristiques génétiques d'une personne ne peut être entrepris qu'à des fins médicales ou de recherche scientifique »*[265]. Plus précisément, l'analyse peut avoir trois objets et notamment *« de rechercher les caractéristiques d'un ou plusieurs gènes susceptibles d'être à l'origine du développement d'une maladie chez une personne ou les membres de sa famille potentiellement concernée »*[266]. Une restriction est posée s'agissant des personnes vulnérables que sont les mineurs et les majeurs sous tutelle puisque pour ces derniers le Code de la santé publique exige qu'ils puissent *« personnellement bénéficier de mesures préventives ou curatives immédiates »*[267].

L'examen ne peut donc avoir pour but que de rechercher une anomalie, d'adapter une prise en charge en fonction des caractéristiques génétiques ou encore de faire évoluer les connaissances en génétique. Au-delà, toute autre

[263] CSP, art. R. 4127-35.
[264] V., M. GUILLET, *op. cit.,* spéc. p. 53 et s.
[265] CSP, art. 16-10 al. 1er.
[266] CSP, art. R. 1131-1, 2°.
[267] CSP, art. R. 1131-4.

utilisation est prohibée[268], comme le rappellent certaines dispositions légales en matière d'assurance ou d'emploi, en raison d'un risque de discrimination[269]. Le domaine des assurances est intéressant en ce que précisément, il conduit à distinguer entre la pathologie déclarée et celle simplement prédite. L'article L. 1141-1 du Code de la santé publique dispose ainsi que *« Les entreprises et organismes qui proposent une garantie des risques d'invalidité ou de décès ne doivent pas tenir compte des résultats de l'examen des caractéristiques génétiques d'une personne demandant à bénéficier de cette garantie, même si ceux-ci leur sont transmis par la personne concernée ou avec son accord. En outre, ils ne peuvent poser aucune question relative aux tests génétiques et à leurs résultats, ni demander à une personne de se soumettre à des tests génétiques avant que ne soit conclu le contrat et pendant toute la durée de celui-ci »*[270]. Le traitement différencié des assurés en fonction de leurs caractéristiques génétiques est donc strictement prohibé. A titre d'exemple, le dépistage de la Chorée de Huntington, anomalie génétique qui entraîne une dégénérescence du système nerveux et dont les premiers symptômes apparaissent vers l'âge de 40 ans, ne peut autoriser l'assureur à opposer un refus assurantiel ou à modifier le calcul des primes d'assurance, quand bien même il s'agirait d'une maladie incurable et de réalisation certaine.

Deux précisions doivent être formulées. Premièrement, le texte interdit à l'assureur de se fonder sur les caractéristiques génétiques de l'assuré mais non de prendre en compte la pathologie d'origine génétique dont les symptômes se seraient déjà déclarés. Deuxièmement, on observe qu'il ne concerne que les caractéristiques génétiques et non d'autres facteurs de prédispositions pathologiques. Ainsi, l'assuré qui souscrit une assurance décès est par exemple tenu de déclarer qu'il est traité pour l'hypertension artérielle ou le diabète, ce qui justifie une augmentation des primes d'assurance en raison d'un risque d'invalidité ou de décès plus élevé. En revanche, il n'a pas à déclarer les

[268] Sous réserve de l'utilisation spécifiquement prévue par d'autres textes, notamment dans le cadre d'une procédure judiciaire.

[269] V., D. DIBIE, « Discriminations biologiques et droits des contrats », *in* Le droit saisi par la biologie, C. LABRUSSE-RIOU, LGDJ, 1996, n° 108, p. 172 ; C. GIRAULT, « Génétique et emploi », *Droit ouvrier*, 2011, n° 750, p. 22 ; I. VACARIE, « Du bon et du mauvais usage des caractéristiques génétiques », *RDSS* 2005, p. 195 ; H. GAUMONT-PRAT, « Les tests génétiques à des fins médicales », in Droits et libertés corporels, *D.* 2012, pan. p. 308.

[270] La même interdiction ressort du droit européen, à l'article 1er de la Convention d'Oviedo, qui dispose plus largement que « *toute forme de discrimination à l'encontre d'une personne en raison de son patrimoine génétique est interdite* ». V., également C. civ, art. 16-13.

anomalies d'origine génétique et ne peut se voir opposer la nullité du contrat pour fausse déclaration en raison de cette omission. Ce régime spécifique réservé aux anomalies génétiques par rapport à d'autres « anomalies » prédisposantes ne va pourtant pas de soi. Alors que l'assuré hypertendu ou diabétique se verra, en effet, opposer une augmentation des primes d'assurances en raison d'un simple *risque* accru de complication de santé, celui qui se sait exposé de manière *certaine* à une pathologie incurable à la suite d'un examen génétique ne s'exposera à aucune différence de traitement. Cette distinction ressort explicitement de l'article 225-3 du Code pénal relatif au délit de discrimination. Ce texte prévoit que ne sont pas punissables les *« discriminations fondées sur l'état de santé, lorsqu'elles consistent en des opérations ayant pour objet la prévention et la couverture du risque décès, des risques portant atteinte à l'intégrité physique de la personne ou des risques d'incapacité de travail ou d'invalidité »* sauf *« lorsqu'elles se fondent sur la prise en compte de tests génétiques prédictifs ayant pour objet une maladie qui n'est pas encore déclarée ou une prédisposition génétique à une maladie »*.

Les caractéristiques génétiques ne peuvent, de même, servir de fondement à un traitement discriminatoire en matière d'emploi, qu'il s'agisse de l'embauche, de l'accès à un stage ou une formation, ou de l'application d'une sanction[271]. *A fortiori*, l'usage de tests génétiques qui viserait d'autres buts que la seule identification d'une pathologie – à l'exception notable de la recherche scientifique - outrepasserait le cadre de la loi, qu'il s'agisse de rechercher le gène du sportif de haut niveau, du délinquant sexuel, de l'individu violent, de l'alcoolique, du toxicomane ou de l'homosexuel[272].

L'utilité. Le fait que le diagnostic – génétique ou non - pratiqué sur une personne soit orienté vers des finalités louables ne dispense pas de s'interroger sur son utilité[273]. Celle-ci va de soi dans une démarche diagnostique classique, qui trouve sa raison d'être dans la plainte d'un individu souffrant. Elle est moins évidente chez un individu ne présentant aucun symptôme. Quelles sont les raisons qui conduisent alors à rechercher une anomalie ? S'agissant de la prescription d'examens génétiques, l'article R. 1131-5 du Code de la santé

[271] C. trav., art. L. 1132-1.
[272] C. DABURON, *op.cit.*
[273] G. GÉRIN, *À propos des applications des recherches sur le génome*, 1995, n° 4, p. 432.

publique envisage deux hypothèses, celle du *« patient présentant un symptôme d'une maladie génétique »* et celle de la *« personne asymptomatique mais présentant des antécédents familiaux »*. C'est donc le critère des antécédents familiaux qui permet de justifier la recherche d'une anomalie génétique chez une personne ne présentant aucun symptôme. Deux cas de figure peuvent se présenter. Soit un ou plusieurs membres de la famille ont présenté une pathologie dont l'origine génétique est suspectée. Soit une anomalie génétique a été détectée chez un membre de la famille et la personne souhaite vérifier si elle en est également affectée. La maladie en cause peut être une affection pour laquelle il existe des solutions de prévention ou non. Dès lors que la personne dispose d'indices laissant penser qu'elle peut être affectée d'une anomalie génétique la prédisposant à une maladie déterminée, c'est à elle de décider si elle souhaite savoir, même s'il n'est pas possible d'agir. C'est le cas, notamment, pour certaines maladies monogéniques incurables.

En revanche, s'agissant du recueil de données secondaires, la question se pose de savoir à quelles pathologies circonscrire la recherche. Les mutations génétiques prédisposantes seront en effet recherchées de manière incidente, sans antécédents familiaux chez la personne ou sans indice permettant de présumer qu'elle en est atteinte. Dans ce cas, l'existence, en l'état de la médecine, de solutions de prévention efficaces, constitue un critère déterminant pour délimiter le champ des anomalies recherchées. Ainsi la liste établie par l'ACMG recommandant, lors du séquençage du génome d'un individu, la recherche de prédispositions, ne concerne que les maladies pour lesquelles une méthode de prévention est disponible. Tel est le cas pour des prédispositions à certains cancers (sein, ovaires, colon, thyroïde) associées à des mutations génétiques identifiées. Pour les pathologies pour lesquelles aucune solution de prévention efficace n'existe, en revanche, la recherche de prédispositions n'apparaît pas utile. Elle pourrait même se révéler nuisible, entraînant des répercussions psychologiques chez l'intéressé, alors même qu'il n'est pas certain que la maladie se déclarera – lorsqu'il s'agit d'une simple prédisposition – et sans possibilité de prévention en amont ni espoir de guérison en aval si finalement la maladie se déclare.

L'enjeu n'est cependant pas le même lorsque le diagnostic porte sur un enfant non encore né, embryon ou fœtus. Lorsqu'il existe un risque de

transmission d'une maladie génétique à l'enfant, le couple ayant un projet parental pourra alors recourir à un diagnostic préimplantatoire (DPI) qui permettra de s'assurer que l'embryon implanté dans l'utérus de la femme n'est pas porteur de l'anomalie génétique. Ce procédé complexe sur le plan technique et suscitant des réserves sur le plan éthique[274] - il est assimilé à une forme d'eugénisme en ce qu'il s'agit de sélectionner un embryon sain – est toutefois strictement encadré. D'une part, le DPI ne peut être réalisé *« qu'à titre exceptionnel »*, le médecin exerçant dans un centre de diagnostic prénatal devant *« attester que le couple, du fait de sa situation familiale, a une forte probabilité de donner naissance à un enfant atteint d'une maladie génétique d'une particulière gravité reconnue comme incurable au moment du diagnostic »*[275]. D'autre part, il suppose qu'ait été *« préalablement et précisément identifiée, chez l'un des parents ou l'un de ses ascendants immédiats dans le cas d'une maladie gravement invalidante, à révélation tardive et mettant prématurément en jeu le pronostic vital, l'anomalie ou les anomalies responsables d'une telle maladie »*[276]. On le voit, c'est ici une logique distincte qui préside puisque le diagnostic prédictif n'est ouvert qu'en présence, notamment, d'une maladie d'origine génétique « incurable ». *A contrario*, s'il s'agit d'une pathologie pour laquelle des soins permettent de prévenir ou traiter efficacement la maladie, le DPI n'est pas justifié et le dépistage se fera lors d'un diagnostic prénatal avec, le cas échéant, mise en œuvre des thérapeutiques actives. Ce qui amène à se pencher sur les suites de la prédiction.

II) Les conséquences de la prédiction

La décision prédictive emporte des conséquences à la fois sur l'information **(A)**, mais aussi sur les méthodes de prévention **(B)** éventuellement mises en œuvre[277].

A) Sur l'information

[274] V., L. LAMBERT-GARREL, *Diagnostic préimplantatoire et diagnostic prénatal*, *in* Les grand avis du CCNE, LGDJ 2013, p. 274 et s.
[275] CSP, art. L. 2131-4 al. 3.
[276] CSP, art. L. 2131-4 al. 4.
[277] Il existe également une incidence sur la procréation. La découverte d'une pathologie génétique grave chez un membre du couple peut les dissuader de procréer ou les amener à recourir au DPI. Le dépistage d'une anomalie génétique grave chez le fœtus peut conduire la femme à demander une interruption médicale de grossesse (IMG).

La prédiction d'une pathologie emporte des incidences sur l'information à plusieurs titres.

L'information délivrée au patient. D'une part, le médecin est tenu d'informer le patient des résultats des analyses effectuées, qu'elles concernent ou non les caractéristiques génétiques, en vertu du droit général de toute personne à être informé sur son *« état de santé »*[278]. S'agissant plus spécialement des résultats d'un dépistage génétique, le Code de la santé publique prévoit une procédure d'information particulière. Ainsi, *« en cas de diagnostic d'une anomalie génétique grave, sauf si la personne a exprimé par écrit sa volonté d'être tenue dans l'ignorance du diagnostic, l'information médicale communiquée est résumée dans un document rédigé de manière loyale, claire et appropriée, signé et remis par le médecin »*[279], la personne attestant de cette remise. En outre, *« Lors de l'annonce de ce diagnostic, le médecin informe la personne de l'existence d'une ou plusieurs associations de malades susceptibles d'apporter des renseignements complémentaires sur l'anomalie génétique diagnostiquée »*.

Rappelons que la faculté pour le médecin de ne retenir une information dans l'intérêt thérapeutique du patient a désormais disparu. L'ancienne formule de l'article R. 4127-35 du code de la santé publique selon laquelle *« dans l'intérêt du malade et pour des raisons légitimes que le praticien apprécie en conscience, un malade peut être tenu dans l'ignorance d'un diagnostic ou d'un pronostic grave, sauf dans les cas où l'affection dont il est atteint expose les tiers à un risque de contamination »* a été supprimée par le décret du 7 mai 2012[280].

En revanche, la personne peut souhaiter ne pas être informée du résultat des tests. Cette faculté est rappelée plus généralement à l'article L. 1111-2 qui dispose que *« La volonté d'une personne d'être tenue dans l'ignorance d'un diagnostic ou d'un pronostic doit être respectée »*. C'est alors à la personne d'apprécier si elle souhaite ou non être informée, au vu de sa capacité à faire face à un éventuel diagnostic ou pronostic défavorable. Une difficulté peut

[278] CSP, art. L. 1111-2.
[279] CSP, art. L. 1131-1-2 al. 2.
[280] V., C. DEBOST, N. GIRODEAU, P. VÉRON, F. VIALLA, « La réforme du code de déontologie médicale », *RGDM* 2012, n° 44, p. 239.

surgir en cas de découverte fortuite, celle-ci devant, à la lecture de la loi, également être révélée au patient. La découverte d'une tumeur à l'occasion d'un examen radiographique ou d'une IRM peut être une chance si elle permet une prise en charge suffisamment précoce. Il est d'autres cas où le bénéfice pour le patient est moins évident. Que penser, par exemple, de la découverte fortuite d'un anévrisme par le biais de l'imagerie cérébrale ? Dans l'hypothèse où une intervention neurochirurgicale est exclue parce qu'excessivement risquée, quel est l'intérêt de faire savoir au patient qu'il est exposé à un risque de rupture d'anévrisme ? La nouvelle ne risque-t-elle pas d'entraîner chez lui un syndrome de stress, qui constitue précisément un facteur aggravant du risque d'accident[281] ? La même difficulté éthique se pose en cas de découverte fortuite de prédispositions génétiques à une maladie. Il est vrai que les progrès des techniques de séquençage du génome permettent aujourd'hui un ciblage précis permettant de limiter ces hypothèses.

Le droit du patient de ne pas être informé trouve toutefois une limite *« lorsque des tiers sont exposés à un risque de transmission »*[282]. La question de l'application de ce texte en matière génétique se pose. Lorsque l'anomalie génétique est héréditaire, peut-on considérer qu'il existe, au sens du texte précité, un risque de transmission à un tiers ? La réponse devrait être négative pour deux raisons. D'une part, le *tiers exposé* à un risque de transmission ne pourrait éventuellement viser que le futur enfant non encore conçu et susceptible d'hériter de l'anomalie, mais il s'agit alors d'un tiers hypothétique. D'autre part, les dispositions spéciales relatives à l'information génétique ne prévoient pas une telle limite. Or, le texte spécial relatif au droit à l'information devrait ici déroger au texte général. La demande de la personne de ne pas savoir doit donc, en matière d'examens génétiques, être respectée sans réserve. En contrepartie, un dispositif spécifique d'information de la parentèle est prévu.

L'information des membres de la famille. La spécificité de l'information génétique est qu'elle peut concerner non seulement la personne qui se soumet au dépistage, mais également les personnes ayant un lien de parenté avec

[281] Sur la question du jugement de proportionnalité en médecine prédictive, Z. GARCIA-LECOEUR, *La proportionnalité en droit de la santé*, thèse, Montpellier, 2014, spéc. n° 451 et s.
[282] CSP, art. L. 1111-2 al. 4.

celle-ci[283]. De manière originale, la loi oblige le patient qui se sait atteint d'une anomalie héréditaire à *« informer les membres de sa famille potentiellement concernés dont elle ou, le cas échéant, son représentant légal possède ou peut obtenir les coordonnées, dès lors que des mesures de prévention ou de soins peuvent leur être proposées »*[284]. Le législateur fait primer l'intérêt collectif de la famille sur la liberté individuelle, mais n'assortit cette obligation d'aucune sanction spécifique. Là encore, cette obligation ne concerne que les maladies pour lesquelles une action, notamment de prévention s'agissant d'un diagnostic prédictif, est envisageable. Toutefois, le médecin peut être autorisé par la personne à informer lui-même les tiers « potentiellement concernés » dans deux cas, soit par que celle-ci n'a pas souhaité être informée, soit parce qu'elle ne souhaite pas procéder elle-même à cette information[285].

B) Sur la prévention

L'un des principaux objectifs du dépistage d'une anomalie génétique est *« d'adapter la prise en charge médicale d'une personne selon ses caractéristiques génétiques »*[286]. Cette prise en charge peut se situer à plusieurs niveaux.

L'hygiène de vie. La découverte d'une prédisposition génétique à une maladie (ex. risque d'accident cardio-vasculaire) peut tout d'abord conduire la personne à modifier ses habitudes de vie[287]. Il convient ici de distinguer les maladies monogéniques – liées au dysfonctionnement d'un gène particulier - des maladies multifactorielles, pour lesquelles la part prédisposante de la mutation génétique incriminée n'est pas toujours parfaitement connue. Pour

[283] N. MILLAIRE, *Le recueil et la diffusion de l'information génétique*, *in* Les grands avis du CCNE, dir. F. VIALLA et E. MARTINEZ, LGDJ 2014, p. 552 et s. ; CCNE, avis n° 76, A propos de l'obligation d'information génétique en matière familiale en cas de nécessité médicale, 24 avr. 2003.

[284] CSP, art. L. 1131-1-3 al. 3.

[285] CSP, art. L. 1131-1-3 al. 4. Un mécanisme similaire est prévu pour la personne atteinte d'une anomalie génétique grave et ayant procédé à un don de gamètes ou d'embryon. L'autorisation peut alors être donnée au médecin prescripteur de *« saisir le responsable du centre d'assistance médicale à la procréation afin qu'il procède à l'information des enfants issus du don »*.

[286] CSP, art. R. 1131-1. C'est pourquoi la génétique est conçue comme l'un des outils de la médecine personnalisée. Sur ce point, H. GAUMONT-PRAT, *La médecine personnalisée et le droit*, Mél. Mémeteau, LEH, 2015, p. 495.

[287] Egalement, à propos des implications de la commercialisation des tests prédictifs par des entreprises privées : X. LABBÉE, « La médecine prédictive et le contrat d'entretien du corps humain », *D*. 2018, p. 2373. Plus largement, M. DEGUERGUE, « L'obligation de mener une vie saine ? », *RGDM*, 2003, n° 11, p. 13.

les pathologies multifactorielles, les facteurs environnementaux joueront bien souvent un rôle déterminant dans le « déclenchement » de la maladie pour laquelle l'individu est génétiquement prédisposé. L'un des rôles des médecins conseillers en génétique est notamment d'orienter les personnes vers des conduites limitant les risques en fonction de leurs caractéristiques personnelles. Certaines des préconisations (activité physique, alimentation saine, limitations de l'alcool et du tabac, régularité du sommeil, etc) sont d'ailleurs celles généralement adressées à l'ensemble de la population dans les messages de santé publique[288].

Le traitement préventif et la délicate question du rapport bénéfice/risque. A un autre niveau, la décision médicale peut être celle de mettre en œuvre un traitement préventif. La question du choix des actes de préventions doit d'une part, être fondée sur les *« données acquises de la science »*[289] ou *« connaissances médicales avérées »* et, d'autre part, ne pas *« faire courir* [au patient] *un risque disproportionné par rapport au bénéfice escompté »*[290]. La première règle de l'éthique médicale hippocratique est, en effet, de ne pas nuire au patient (*primum non nocere* ou règle de la raison proportionnée). L'évaluation du rapport bénéfice/risque peut apparaître particulièrement délicate en matière de médecine prédictive, lorsqu'il s'agit de décider de l'opportunité de mettre en œuvre un traitement mutilant (mastectomie, colectomie) ou comportant lui-même des risques ou effets secondaires lourds (irradiation, séquelles neurologiques, paralysie, insuffisance musculaire, etc), afin de prévenir une pathologie dont l'avènement n'a rien de certain mais repose sur des probabilités plus ou moins bien établies.

Les décisions d'intervention préventive en oncogénétique - cancers d'origine génétique, en particulier cas de cancers familiaux - fournissent sur ce point d'intéressantes illustrations. Pour prendre une décision, les médecins spécialistes de la discipline s'appuient aujourd'hui sur des critères nationaux et internationaux contenus dans des référentiels. Des logiciels d'aide à la décision

[288] S'agissant du dépistage et du traitement de maladies communes (hypertension, diabète, hypercholestérolémie), la valeur ajoutée des analyses génétiques pour le patient est parfois questionnée, dès lors que la manière de détecter et de traiter ces affections, et ainsi prévenir le risque d'accident, est bien maîtrisée. Elle aurait, tout au plus, un intérêt sur le plan de l'avancée des connaissances sur l'origine de ces pathologies.

[289] CSP, art. R. 4127-32.

[290] CSP, art. L. 1110-5.

sont également utilisés pour préciser la probabilité d'une prédisposition génétique en tenant compte de divers paramètres tels que le degré de parenté des personnes atteintes, l'âge de déclaration de la maladie chez ces derniers ou encore l'existence de comorbidités.

Il existe aujourd'hui plus de cinquante gènes identifiés dont les mutations sont associées à des prédispositions de cancer et les études montrent ainsi que le risque de développement d'un cancer est souvent très élevé chez les personnes porteuses d'un gène de susceptibilité[291]. Plusieurs exemples permettent d'illustrer les paramètres de la décision préventive en oncogénétique[292].

Ainsi, pour les cancers médullaires familiaux de la thyroïde, l'indication est la thyroïdectomie préventive, geste considéré comme acceptable en termes de qualité de vie même s'il implique la prise rigoureuse d'un traitement à vie[293].

Pour d'autres cancers, la recommandation consiste, en priorité, dans une surveillance accrue. Ainsi, en présence d'un gène prédisposant au cancer du côlon, la surveillance consistera dans des coloscopies régulières (tous les 2 ans à partir de 20 ans) et le dépistage – avec le cas échéant l'exérèse - des lésions précancéreuses[294].

Pour une prédisposition à un cancer du sein (gène BRCA 1 et 2), les recommandations consistent dans un examen clinique biannuel (débuté à l'âge de 20-25 ans) une mammographie, une échographie et une IRM annuelles (débutée entre 25 et 30 ans). En revanche, lorsqu'une tumeur cancéreuse s'est déclarée sur un sein, les statistiques montrent que le risque d'apparition d'un cancer sur l'autre est estimé à 50%. La mastectomie bilatérale préventive est parfois recommandée dans ce cas, notamment lorsqu'il existe de nombreux cas

[291] Pour le cancer du sein ou du colon, la prédisposition génétique entraîne un risque de 50% à 70%. Pour d'autres cancers héréditaires, le risque est de presque 100% (rétinoblastome, cancre médullaire de la thyroïde, polypose adénomateuse familiale.

[292] Nous nous appuyons ici sur l'étude de P. PUJOL, « La médecine prédictive », *préc.*

[293] La mutation prédisposante est le gène RET considéré comme responsable de la quasi-totalité des cas familiaux et le risque de cancer de 100% à l'âge de 40 ans.

[294] Le risque de cancer chez l'individu porteur de la mutation génétique est de 50 à 60%. Des cancers surviennent avant l'âge de 50 ans, parfois avant l'âge de 30 ans, c'est pourquoi une surveillance précoce s'impose. En revanche, au vu de la probabilité de survenance de la maladie, l'ablation du colon (colectomie préventive) n'est généralement pas retenue.

familiaux. L'ablation préventive des seins sera alors pratiquée sans pourtant qu'il soit possible de savoir si un cancer se serait ou non déclaré.

Enfin, d'autres mutations génétiques exposent à un cancer difficilement curable même en cas de dépistage précoce. Tel est le cas du cancer ovarien. En revanche, la mutation génétique n'entraine un risque de développement du cancer que pour un taux de 30%, moins élevé que pour le cancer du sein. La recommandation est malgré tout l'ovariectomie chez les femmes de plus de 40 ans BRCA1 et BRCA2.

On le voit, les implications de la prédiction sont importantes. Elles peuvent avoir des répercussions à la fois physiques et psychiques sur l'intéressé[295].

Le recours aux systèmes d'aide à la décision. La promotion du modèle de la médecine des preuves (*evidence based medicine*) induit notamment le recours croissant, dans différentes spécialités médicales, aux logiciels d'aide à la décision[296]. On distingue notamment l'aide à la prescription de l'aide au diagnostic. Certains de ces outils, qui reposent sur des algorithmes complexes, sont prédictifs. On peut prendre l'exemple du logiciel « Adjuvant ! Online », créé aux Etats-Unis en 2001. Son objectif est d'aider les médecins à décider d'un traitement post-opératoire par chimiothérapie ou hormonothérapie chez une femme opérée d'un cancer du sein, sur la base de plusieurs paramètres pronostiques. Le logiciel sert ainsi à modéliser le devenir de la patiente sous forme de probabilité de rechute tumorale et de mortalité liée au cancer. Au terme d'une simulation, il est censé déterminer la plus-value clinique de l'ajout d'un traitement au regard du pronostic.

Si l'utilité de ces logiciels est reconnue, les biais éthiques qu'ils comportent ont pu être soulignés : *« la forme informatique n'est, en réalité, pas neutre pour le processus de décision médicale. La décision ne se contente pas d'être affinée par la présentation de connaissances à jour* (…). *Un clic et le logiciel nous dira instantanément si oui ou non la patiente opérée d'un cancer du sein tirera plus de bénéfices que de dommages à être traitée par une chimiothérapie lourde.*

[295] L'opportunité d'une intervention est encore moins évidente pour les patientes porteuses de la mutation génétique mais sans antécédents personnels ou familiaux. Pour ces dernières, les données, basées pour l'essentiel des cas de cancers familiaux, ne permettent pas d'évaluer l'existence d'un sur-risque par rapport à la population générale.

[296] M. CLÉRET, P. LE BEUX, F. LE DUFF, « Les systèmes d'aide à la décision médicale », *Les Cahiers du numérique*, 2001/2, vol. 2 p. 125.

L'informatique tranchera. Elle tranchera vite. Et elle tranchera une question insoluble face à une incertitude radicale »[297]. Les auteurs ajoutent : *« Les logiciels d'aide à la décision affectent le rapport du décideur médical aux connaissances scientifiques. Le surgissement de leurs résultats suscite un sentiment d'évidence quant à leur nature, leur existence et donc leur légitimité »*[298].

L'immédiateté et la précision du résultat fourni par un logiciel ne doivent pas conduire à négliger le temps d'échange avec le patient et la question des préférences de ce dernier, notamment les contraintes liées aux soins qu'il est prêt à accepter. Une autre interrogation concerne le contenu des bases de données sur lesquelles ces logiciels se fondent pour fournir leurs résultats[299]. Pour l'essentiel, les praticiens utilisent ces logiciels sans savoir à partir de quelles bases de données – cas cliniques, études statistiques – ils sont élaborés et alimentés, ni comment raisonne l'algorithme. La loi n'impose aucune obligation de formation en la matière. La compréhension de cet outil complexe apparaît pourtant un enjeu important pour que le décideur médical conserve une juste distance critique à l'égard des résultats normatifs qu'ils fournissent[300]. C'est d'autant plus le cas lorsque ces résultats consistent dans la préconisation d'un traitement préventif mutilant ou risqué face à un risque pathologique.

[297] A. et E. KEMPF, « L'informatisation de l'aide à la décision : la décision médicale est-elle indemne ? L'exemple d'un outil prédictif en cancérologie », *Revue française d'éthique appliquée*, 2016/1, p. 59.
[298] *Ibid.*
[299] C. SYBORD, « *Big Data* et conception d'un système d'informatisation d'aide à la médicale », *Les Cahiers du numérique*, 2016/1, vol. 12, p. 73.
[300] V., D. Le METAYER, S. DESMOULIN-CANSELIER, « Gouverner les algorithmes pour éviter qu'ils nous gouvernent », Libération, 26 novembre 2017 ; Y. POULLET, « Le droit face aux développements de l'intelligence artificielle dans le domaine de la santé », *Revue Lamy Droit de l'immatériel*, 2018, n° 152, p. 43.

Les drones et l'ordre public : entre optimisation de la prévention des infractions et sauvegarde des libertés fondamentales

Laurène BAUDOUIN

Doctorante en droit Université de Lille,
CERAPS-UMR CNRS 8026

Marcel MORITZ

Maître de conférences, HDR
Université de Lille,
CERAPS-UMR CNRS 8026

En réponse notamment aux attaques terroristes que la France a connu ces dernières années, de nouveaux dispositifs technologiques ont progressivement été mis en place. L'usage d'outils numériques de prévention et de répression des infractions s'étend, induisant une polémique quant aux incidences que ces technologies peuvent engendrer sur les libertés fondamentales.

Si la modernisation des outils de surveillance est loin d'être une nouveauté, leur expansion renouvèle les questionnements juridiques. Dans la continuité des dispositifs bien connus de vidéoprotection fixes, les drones sont désormais considérés par certains comme une extension pertinente du domaine de la surveillance. D'une part, leur mobilité leur confère un fort atout puisqu'ils accèderont à des zones qui demeurent jusqu'alors inaccessibles et offriront une vue plus extensive et plus précise que ne le font les dispositifs fixes de vidéoprotection. D'autre part, la possibilité d'être en mesure d'équiper ces drones de nombreux capteurs augmentera leur efficacité dans le cadre de missions de sécurité publique. Toutefois, l'acceptabilité de l'usage de tels outils, tant sur le plan juridique que sur le plan social, nécessitera un cadre juridique protecteur des droits des individus. Au-delà des aspects liés à l'extension du domaine de la vidéoprotection et de la possible fragilisation des

libertés individuelles induite **(I)**, l'introduction d'algorithmes de détection de comportements anormaux associés à ces drones interpelle le juriste **(II)**.

I) Les drones comme nouveaux dispositifs de vidéoprotection (par Laurène Baudouin)

En vue d'assurer la sécurité des individus sur le territoire national, le législateur a permis aux agents des forces de l'ordre de recourir à des outils de surveillance destinés à collecter des données en vue de prévenir et de sanctionner toute forme d'infraction. Au fil des années, ces dispositifs de surveillance se sont diversifiés. Ils sont en nette croissance, en concordance avec la politique actuelle de renforcement de la sécurité introduisant de nouvelles mesures défavorables à l'expression des libertés dans l'espace public. Parmi les moyens permettant d'assurer la sécurité des individus, les drones intéressent les forces de l'ordre en raison de leur capacité à collecter et enregistrer des images par le biais de caméras, à capter des sons ainsi que de nombreux autres types de données afin de recueillir des informations.

Autrefois, relevant des technologies militaires les plus coûteuses et complexes, les drones se sont profondément démocratisés, passant d'engin militaire à gadget de divertissement, et trouvant une application sur-mesure en matière de surveillance. Ces drones entrent dans le cadre des dispositifs de vidéoprotection, définis par la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure[301] dite *Loppsi 2* et par le Code de la sécurité intérieure, et devront par conséquent, répondre aux exigences qui y sont liées. Or, le respect des conditions issues des textes relatifs à la vidéoprotection soulève des difficultés particulières s'agissant des drones.

Les drones destinés aux forces de police et de gendarmerie ont pour objectif de maintenir l'ordre public. La sécurité publique se trouve au cœur de l'ordre public et n'a vocation à s'exprimer que sur le territoire national, contrairement à la sécurité nationale qui dispose d'un champ plus étendu. Or, les textes juridiques destinés à préserver l'ordre public semblent désormais dépasser le

[301] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, *JO* n°0062 du 15 mars 2011, page 4582, texte n° 2 https://www.legifrance.gouv.fr/eli/loi/2011/3/14/IOCX0903274L/jo#JORFSCTA000023707348

simple cadre du territoire national ; tel est notamment le cas dans le cadre de la loi du 24 juillet 2015 relative au renseignement[302] qui ne se limite pas uniquement à la lutte contre le terrorisme. En d'autres termes, la distinction entre sécurité publique et sécurité nationale devient de plus en plus ténue à mesure que les actes de grand banditisme et de terrorisme gagnent du terrain et ne se limitent pas à un territoire mais dépassent les frontières des États, qu'elles soient physiques ou virtuelles. En conséquence, les règles juridiques tenant à la sécurité intérieure des États voient leur champ d'action s'étendre, offrant davantage de prérogatives aux forces de l'ordre **(A)**. Ces dispositions juridiques leurs confèrent une plus grande liberté d'action, qui n'est cependant pas sans conséquences sur les libertés fondamentales des individus **(B)**.

A) La justification d'un usage accru des outils de vidéoprotection

L'ordre public se fonde sur l'obligation de l'État de protéger les droits des individus et traduit, par conséquent, la nécessité d'assurer la sécurité et le respect des libertés de chacun. De fait, la sécurité des personnes et des biens « *est une des composantes identifiées de l'objectif de sauvegarde de l'ordre public* »[303] et s'associe à la prévention de certaines infractions. Aussi, l'État, dans l'exercice de son devoir de sécurité, doit remplir une obligation d'anticipation des menaces. Afin de mener à bien cette obligation de prévention, le législateur a complété les dispositions en matière de police destinées à sauvegarder l'ordre public ou visant la recherche de l'auteur d'une infraction, par des moyens de police administrative ayant vocation à prévenir la commission de certaines infractions déterminées[304]. Les dispositifs de vidéoprotection constituent une expression de ces moyens octroyés aux forces de l'ordre, fondés sur la prévention de certaines infractions. L'efficacité de ces dispositifs est invoquée pour justifier leur déploiement et la place essentielle qu'ils occupent désormais dans l'exécution des missions de sécurité publique. Les systèmes de vidéoprotection assurant la surveillance des espaces publics poursuivent un objectif global de sécurité des personnes sur le territoire

[302] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, *JO* n°0171 du 26 juillet 2015 page 12735 texte n° 2 https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorieLien=id
[303] GRANGER, Marc-Antoine, *Constitution et Sécurité Intérieure : Essai de modélisation juridique*, Éditions LGDJ, Paris, 2011, p. 193.
[304] *Ibid*.

national, en d'autres termes, ils ne visent pas les personnes de manière individuelle mais l'ensemble de la population. Ces dernières années, la politique de sécurité intérieure se concentre principalement sur la protection du collectif privilégiant les libertés publiques aux libertés individuelles. En conséquence, l'équilibre fragile entre sécurité et liberté voit sa balance pencher en faveur d'un renforcement de la surveillance censée prévenir les actes de délinquance et de terrorisme. Les attentats survenus en 2015 ont favorisé et renforcé la légitimité des dispositifs de contrôle[305]. Les drones font partie intégrante de cet accroissement de la surveillance en ce qu'ils permettent de collecter une plus grande quantité de données, amplifiant le phénomène de surveillance justifié par les besoins de prévention et de répression des infractions.

Parmi les données collectées par les drones, certaines sont des données à caractère personnel, encadrées par la loi du 6 janvier 1978, dite « Informatique et Libertés »[306], ayant récemment fait l'objet d'une réadaptation[307] suite à l'entrée en vigueur en mai 2018 du Règlement général sur la protection des données (RGPD) du 27 avril 2016[308] et de la Directive relative à la protection des données dans le domaine pénal, dite « Police-Justice »[309]. Les données à caractère personnel sont définies par l'article 2 de la loi Informatique et Libertés et font référence à toutes les données permettant, directement ou indirectement, d'identifier ou de rendre identifiable un individu. Bien qu'il puisse se justifier, le traitement de données à caractère personnel issues des

[305] H. ALCARAZ, « Faut-il avoir peur de la loi sur le renseignement ? Entre risque d'ingérence et « illusion technologique », p. 121, issu de *Protection des données personnelles et Sécurité nationale : Quelles garanties juridiques dans l'utilisation du numérique ?*, sous la coordination de O. DE DAVID BEAUREGARD-BERTHIER et Akila TALEB-KARLSSON, Éditions Bruylant, Bruxelles, 2017, 279 p.

[306] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JO* du 7 janvier 1978 page 227. [https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460].

[307] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, *JO* du 21 juin 2018 [https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=2C3701405346AB2F8535D020C12CC702.tplgfr23s_2?cidTexte=JORFTEXT000037085952&dateTexte=20180621].

[308] Règlement (UE) n°2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *JO* L 119, 4 Mai 2016, pp. 1–88 [http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR].

[309] Directive (UE) n°2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, *JO* L 119, 4 mai 2016, pp. 89-131 [https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016L0680&from=FR]

drones constitue une forme d'immixtion de l'État dans la vie privée[310]. Pour autant les États conservent des intérêts légitimes à traiter des données à caractère personnel, le principal motif étant celui de la sécurité. Toutefois, le Conseil constitutionnel subordonne le droit au traitement de ces données par la justification du caractère constitutionnel des mesures dans lequel entre la sauvegarde de l'ordre public. Les atteintes à l'ordre public permettent de justifier ce recours aux traitements de données à caractère personnel. De fait, ces données peuvent s'avérer capitales tant dans le cadre des activités de prévention que de répression des infractions permettant la recherche d'individus. Afin de faciliter ces recherches, les données à caractère personnel collectées sont interconnectées avec des données de géolocalisation par le biais d'outils GPS. Au préalable, le législateur a mis en œuvre un cadre d'utilisation de ces outils de géolocalisation[311] qui sont soumis au contrôle de l'autorité judiciaire. Enfin, le traitement de données à caractère personnel aura permis la création de fichiers, notamment judiciaires, qui s'avèrent essentiels lors de recherches d'identification de l'individu responsable d'un délit ou d'un crime. Ces fichiers renferment des bases de données qui peuvent être interconnectées. Or, l'interconnexion de ces fichiers permet d'obtenir une information plus précise sur chaque individu et ce plus particulièrement lorsque ces données, qui prises individuellement, semblent en apparence peu significatives concernant la vie et les habitudes d'une personne mais qui par croisement offrent la possibilité d'établir un profil de celle-ci[312]. Cette opportunité d'interconnexion des données incite à collecter davantage de données dans l'éventualité où celles-ci pourraient s'avérer utiles au maintien de l'ordre public. L'État suit une tendance allant vers une multiplication des données collectées et continue d'y être favorable comme le traduit notamment la loi sur le renseignement de 2015. Cette loi permet une extension du champ des données collectées ainsi qu'une plus grande précision des informations sur un individu puisqu'elle ouvre un droit de collecte de données en temps réel qui s'étend aux personnes présentant des liens étroits et susceptibles de livrer des

[310] C. CERDA-GUZMAN, « La position des États à l'égard des données personnelles : entre velléité d'utilisation et obligation de protection » p. 39, issu de *Protection des données personnelles et Sécurité nationale : Quelles garanties juridiques dans l'utilisation du numérique ?*, sous la coordination de O. DE DAVID BEAUREGARD-BERTHIER et A. TALEB-KARLSSON, Éditions Bruylant, Bruxelles, 2017, 279 p.

[311] Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation, *JO* n°0075 du 29 mars 2014 page 6123 texte n° 1 [https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028790796&categorieLien=id].

[312] C. CERDA-GUZMAN, « La position des États à l'égard des données personnelles : entre velléité d'utilisation et obligation de protection » pp. 46-47, *op.cit*.

informations sur la personne ciblée. Naturellement, l'intérêt de la puissance publique pour l'utilisation de drones de sécurité ne fait que traduire cette volonté de l'État d'accéder à un volume toujours plus important de données.

Les préoccupations de sécurité et les besoins en matière de données à caractère personnel ont également suscité l'intérêt de l'Union européenne, qui se reflète à travers la nouvelle directive de protection des données en matière pénale[313] intéressant directement les forces de l'ordre. Cette directive reprend pour l'essentiel les dispositions énoncées par le RGPD sans pour autant l'égaler. La directive « police-justice » apporte ainsi une avancée significative en matière de traitement de données dans le cadre pénal en favorisant les échanges entre les autorités publiques des États, enjeu devenu essentiel à la lutte contre le terrorisme et la criminalité[314]. Elle reprend la quasi-totalité des principes de protection des données à caractère personnel énoncés par le RGPD en omettant, néanmoins, celui relatif à la transparence liée à la collecte de ces données qui peut toutefois s'expliquer compte tenu de la teneur du texte. Enfin, ce texte prend en compte les évolutions technologiques nécessitant une plus ample protection des données et pourra s'appliquer aux différents dispositifs de surveillance.

Le maintien de l'ordre public semble justifier l'utilisation d'outils de surveillance tels que les drones mais requiert, cependant, de prendre certaines précautions en vue d'assurer la sécurité des données à caractère personnel et, de manière globale, de préserver les libertés fondamentales des individus.

B) La possible fragilisation des libertés fondamentales

Les libertés fondamentales deviendront-elles bientôt une illusion à mesure que les technologies de surveillance destinées à assurer la sécurité publique se généraliseront, en toute circonstance et sur l'ensemble du territoire national ? La discrétion permise par les drones nécessite d'insister plus lourdement sur la

[313] Directive (UE) n°2016/680 du 27 avril 2016, *op. cit.*

[314] S. PEYROU, « La Directive 2016/680 du 27 avril 2016 (protection des données dans les domaines de la coopération policière et judiciaire en matière pénale », p. 466, issu de *L'échange des données dans l'Espace de liberté, de sécurité et de justice de l'Union européenne*, sous la direction de C. CHEVALLIER-GOVERS, Éditions Mare & Martin, Grenoble, 2017, 559 p.

question du respect des libertés fondamentales. En vue de préserver ces libertés, certaines garanties ont été mises en place sous la forme d'autorités administratives indépendantes et de l'encadrement des autorités juridictionnelles. Toutefois, la réalité des garanties apportées aux citoyens dans un contexte de lutte antiterroriste est parfois à nuancer. À titre d'exemple, il est utile de rappeler la décision rendue par le Conseil d'État le 18 octobre 2018[315] rejetant les requêtes émises contre le décret instituant le mégafichier TES (Titres électroniques sécurisés), regroupant l'ensemble des données personnelles de tous les Français, comme constituant une atteinte disproportionnée aux libertés des personnes. Pourtant, la fusion de ces fichiers de données personnelles des Français met l'ensemble des individus sur un pied d'égalité, en regroupant ceux constitués à des fins policières comme ceux de recensement administratif, autrement dit, les recherches ne seront plus restreintes à certains individus mais cibleront l'ensemble de la population française. La CNIL, quant à elle, s'est vue accorder un pouvoir de contrôle plus important sur les données à caractère personnel à mesure que se multiplient les lois relatives aux activités de surveillance. Mais cette évolution permet-elle véritablement d'assurer le respect de la vie privée et des données personnelles dans le cas des drones ? L'intérêt prononcé des États pour le recours massif aux données à caractère personnel présente deux risques majeurs : d'une part, celui porté aux libertés fondatrices d'un État démocratique, et, d'autre part, le risque de cyberattaques pouvant atteindre ces données, la sécurité de l'État reposant, en partie, sur ces dernières[316].

Au nombre des usages permis par les drones, la surveillance des manifestions participe aux différents objectifs visés dans le cadre du maintien de l'ordre public[317]. L'emploi de drones serait alors susceptible d'entraver l'expression de la liberté de manifestation qui, comme le rappelle le Conseil d'État dans une décision du 26 juillet 2014[318], appartient aux libertés fondamentales et à ce titre doit être conciliée avec la préservation de l'ordre public. La liberté d'aller et venir entre également dans le champ des libertés

[315] CE, 10ème et 9ème ch., 18 octobre 2018, n°404996.
[316] C. CERDA-GUZMAN, « La position des États à l'égard des données personnelles : entre velléité d'utilisation et obligation de protection » p. 51, *op.cit*.
[317] J. SIBER, « L'image et le manifestant », n°4, *Gaz. Pal.*, 24 janvier 2017, p. 81.
[318] CE, ord. réf., 26 juillet 2014, *M. C... et autres*, n°383091.

fondamentales entravées par les systèmes de vidéoprotection et serait d'autant plus fragilisée que les drones amplifieront le phénomène d'observation des individus. La liberté de circuler librement et anonymement sur et en dehors du territoire serait en un sens soumise à conditions[319], or, la CNIL rappelait, en 2003 déjà, que l'anonymat est une « *condition nécessaire de la liberté d'aller et venir* » et que « *les technologies de radio-identification ou étiquettes intelligentes montrent le risque de suivi des individus qui en sont porteurs* »[320].

Par ailleurs, la facilitation par la directive « police-justice » de la captation de données à caractère personnel de même que leur transmission entre autorités publiques des différents États membres de l'Union européenne à des fins de sécurité n'est pas favorable à l'exercice du droit à la vie privée. La directive énonce que les États devront assurer la protection des droits et des libertés fondamentaux en visant plus spécifiquement la protection des données à caractère personnel[321]. Néanmoins, elle ajoute que les données peuvent faire l'objet d'un traitement à des fins de prévention et de détection des infractions pénales « *contre les menaces pour la sécurité publique et la prévention de telles menaces* »[322]. Le champ d'action des forces de l'ordre n'est donc pas précisément défini, laissant une incertitude quant aux circonstances dans lesquelles la collecte de données pourrait s'effectuer. Concernant le principe de minimisation des données, la directive fait preuve de plus de souplesse que le RGPD, qui exige que les données collectées soient « *limitées* », et requiert uniquement que ces données soient « *non excessives* » octroyant un plus grand pouvoir de collecte aux forces de l'ordre. De même, le principe de finalité du traitement demeure assez obscur en permettant, dans certaines conditions, le traitement de données pour des finalités autres que celles pour lesquelles elles ont été collectées[323]. Le défaut de transparence et les possibilités larges de collecte de données à caractère personnel accordés aux institutions publiques

[319] R. HANICOTTE, « Une nouvelle catégorie d'OVNI juridique: les drones », n°317, *Gaz. Pal.*, 13 novembre 2014, p. 6.
[320] CNIL, « 24ème rapport d'activité 2003 », Paris, *La Documentation française*, 2004, 539 p., p. 135 [https://www.cnil.fr/sites/default/files/typo/document/Cnil24_Docfr.pdf].
[321] Directive (UE) n°2016/680 du 27 avril 2016, *op. cit.*, art. 1er.
[322] *Ibid*.
[323] *Idem*, art. 4§2.

par la directive créent donc une inquiétude légitime quant au sort réservé aux libertés.

En cas d'atteinte disproportionnée aux libertés fondamentales du fait de l'utilisation de drones de sécurité publique, il sera possible de saisir les autorités administratives et juridictionnelles compétentes. Mais encore faudra-il que le justiciable soit au fait des droits dont il dispose. Or, le devoir d'information applicable à l'usage des systèmes de vidéoprotection est largement théorique en matière de drones. Ainsi, comment répondre à des situations d'urgence tout en assurant une information préalable de leur usage ? Leur mobilité ainsi que leur miniaturisation ne sont-ils pas des facteurs allant à l'encontre de cette obligation d'information ? Les dispositions supposées protéger les libertés fondamentales semblent, par conséquent, ne plus suffire dans le cas des drones à l'usage des forces de l'ordre.

La quantité de données que peuvent collecter les drones en font des outils de surveillance de masse ouvrant aux seuls services des forces de l'ordre une connaissance des informations recueillies dont ne bénéficient pas les personnes concernées. Cet état d' « ignorance » du justiciable – bien que nécessaire à l'efficacité du renseignement - engendre par ailleurs une carence quant au respect du principe du contradictoire et créé un potentiel déséquilibre dans ce qui devrait être un procès équitable. Cet état de fait démontre la fragilité de l'exercice des droits fondamentaux.

Enfin, l'usage massif de données à caractère personnel nécessite de prendre les mesures adéquates permettant d'assurer leur sécurité contre toute forme de piratage préservant par conséquent la sécurité de l'État, lui-même. De fait, les États ne sont pas à l'abri d'une attaque visant les données à caractère personnel. Pour prévenir ces atteintes aux données, il importe de limiter leur collecte, le risque s'accentuant à mesure que s'accumulent les données qui lorsqu'elles sont interconnectées peuvent s'avérer fournir des informations essentielles relatives à la sécurité de l'État. Un autre argument en faveur de la limitation de la captation de données tient aux risques présents au sein même des institutions de l'État, la transmission de ces données d'un service à un autre créant une diminution de la protection de celles-ci.

Le besoin de préserver les libertés fondamentales repose ainsi sur la volonté de maintenir un État démocratique et participe aussi indirectement à la sauvegarde de l'ordre public. Il convient de rappeler à cet égard que l'ordre public inclut également la sûreté, qui peut se définir comme la garantie dont dispose chaque être humain contre l'arbitraire du pouvoir. Mais les outils de vidéoprotection ne se limitent pas à la collecte de données et seront très prochainement en mesure de prendre des décisions de manière automatisée sur base d'algorithmes de détermination du comportement des personnes permettant de constater, voire de prédire, les infractions, ce qui soulève de nouvelles questions de droit.

II) Les outils algorithmiques d'aide à la prévention des infractions associés aux drones (par Marcel Moritz)

Les drones permettent de capter un volume massif d'images qui viennent s'ajouter à l'ensemble de celles collectées par les autres dispositifs de vidéoprotection (caméras fixes, caméras orientables, caméras mobiles placées sur les agents, etc.). De fait, l'analyse en temps réel de ces images par les personnels des forces de l'ordre devient de plus en plus difficile, pour ne pas dire impossible. Fort logiquement, des outils algorithmiques d'aide à la prévention des infractions ont donc naturellement vocation à renforcer l'efficacité de la surveillance permise par les drones en analysant les images et en attirant l'attention des agents sur les seuls comportements suspects. De tels logiciels de détection de comportement anormaux ne constituent pas en tant que tels une nouveauté, puisque leurs enjeux juridiques et sociaux sont questionnés depuis plusieurs années déjà[324]. Mais la mise en œuvre de ces technologies va très probablement s'amplifier avec l'usage des drones de sécurité, dont le déploiement constitue un enjeu économique majeur pour les entreprises qui les développent. Cela ne manque pas d'interroger quant au régime juridique des outils algorithmiques associés **(A)** mais aussi aux délégations de service public que cette technologie permet **(B)**.

[324] V. notamment sur le projet Canada (Comportements Anormaux : Analyse, Détection, Alerte) : J-J. LAVENUE, et B. VILLALBA, (dir.), *Vidéo-surveillance et détection automatique des comportements anormaux : Enjeux techniques et politiques*, éd. Septentrion, 2011, 294 p.

A) La question du régime juridique des outils algorithmiques associés aux systèmes de vidéoprotection

Depuis la fin des années 1970, la transparence administrative a été érigée en un principe important : transparence relative aux fichiers informatiques avec la célèbre loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ou encore transparence liée au libre accès aux documents administratifs avec la tout aussi célèbre loi n° 78-753 du 17 juillet 1978.

Plus récemment, le déploiement des algorithmes au sein de l'administration a permis de renouveler les débats autour de cette nécessaire transparence[325], interrogeant quant à une éventuelle évolution de la tétralogie traditionnelle des « lois » du service public (égalité, continuité, neutralité et mutabilité), que la transparence viendrait rejoindre. Soulignons toutefois que le Conseil d'État a refusé la reconnaissance d'un principe général de transparence[326] et que son rapport annuel 2017 va même plus loin, précisant s'agissant spécifiquement des algorithmes que ceux « *utilisés par les administrations publiques dans le cadre de l'exercice de leurs missions pourraient sans doute, lorsque cela est possible, faire l'objet d'une transparence plus grande du fait des implications normales du droit à une bonne administration que sont l'accès des personnes à leur dossier et la motivation des décisions administratives* »[327], mais que « *l'affirmation d'un principe de transparence des algorithmes n'a (...) plus véritablement de sens. Elle nuirait en outre au respect du secret industriel et pourrait potentiellement freiner l'innovation* »[328]. Cette absence de principe général n'exclut pas toutefois le développement récent de dispositions visant à garantir une transparence accrue quant au fonctionnement des algorithmes. Depuis la loi pour une République numérique du 7 octobre 2016, il est ainsi précisé à l'article L. 312-1-3 du Code des relations entre le public et l'administration (CRPA) que, sauf exception, les administrations « *publient en ligne les règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions*

[325] V. F. GRABIAS, « La transparence administrative, un nouveau principe ? », *JCP A*, n°50, 17 décembre 2018, 2340.
[326] CE, 23 février 2005, n° 241796, Ass. coordination nationale Natura 2000.
[327] Rapport 2017 du Conseil d'État, « Puissance publique et plateformes numériques : accompagner l'«ubérisation» », p.116.
[328] *Ibid*.

individuelles ». La partie règlementaire du même Code souligne, quant à elle, l'importance de procéder à une communication à la fois complète et réellement exploitable par les personnes intéressées. L'article R. 311-3-1-2 du CRPA précise ainsi que « *L'administration communique à la personne faisant l'objet d'une décision individuelle prise sur le fondement d'un traitement algorithmique, à la demande de celle-ci, sous une forme intelligible et sous réserve de ne pas porter atteinte à des secrets protégés par la loi, les informations suivantes : 1° Le degré et le mode de contribution du traitement algorithmique à la prise de décision ; 2° Les données traitées et leurs sources ; 3° Les paramètres de traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé ; 4° Les opérations effectuées par le traitement* ».

S'agissant spécifiquement d'algorithmes de détection de comportements anormaux associés aux drones de sécurité, une réserve majeure s'impose cependant. En effet, l'article R. 312-1-3 du CRPA précité ne s'applique pas aux secrets protégés en application du 2° de l'article L. 311-5. Or figurent parmi ces secrets le « secret de la défense nationale », ou encore les documents dont la consultation ou la communication porterait atteinte à la « *sûreté de l'État, à la sécurité publique, à la sécurité des personnes ou à la sécurité des systèmes d'information des administrations* ». Si l'interprétation de ces dispositions relève de l'approche souveraine des juges du fond, il apparaît donc que la transparence algorithmique trouve ici des limites essentielles. Ces limites sont à de nombreux égards aisément compréhensibles, une connaissance trop fine du fonctionnement de l'algorithme pouvant conduire à son contournement. Toutefois, cette limitation soulève la question - essentielle - de l'acceptabilité sociale d'un tel contrôle à la fois diffus et potentiellement opaque. Cette problématique est d'autant plus cruciale qu'il en va de la confiance même des usagers dans les institutions publiques qui font usage de ces technologies. C'est la raison pour laquelle le Conseil constitutionnel a souligné dans sa décision du 12 juin 2018[329] « *que, lorsque les principes de fonctionnement d'un algorithme ne peuvent être communiqués sans porter atteinte à l'un des secrets ou intérêts énoncés au 2° de l'article L. 311-5 du code des relations entre le public et l'administration, aucune décision individuelle ne peut être prise sur le*

[329] Cons. const. 12 juin 2018 n° 2018-765 DC du 12 juin 2018, Loi relative à la protection des données personnelles, cons. 70.

fondement exclusif de cet algorithme. D'autre part, la décision administrative individuelle doit pouvoir faire l'objet de recours administratifs, conformément au chapitre premier du titre premier du livre quatrième du code des relations entre le public et l'administration. L'administration sollicitée à l'occasion de ces recours est alors tenue de se prononcer sans pouvoir se fonder exclusivement sur l'algorithme. La décision administrative est en outre, en cas de recours contentieux, placée sous le contrôle du juge, qui est susceptible d'exiger de l'administration la communication des caractéristiques de l'algorithme. Enfin, le recours exclusif à un algorithme est exclu si ce traitement porte sur l'une des données sensibles », ce qui inclut donc les données biométriques.

Un certain nombre de mesures protectrices ont ainsi été posées. Mais il nous semble que dans un État de Droit, au-delà de ces enjeux, la garantie la plus importante doit demeurer la maîtrise par la personne publique du fonctionnement de l'algorithme.

B) La question de la maîtrise de la personne publique sur le fonctionnement de l'algorithme

De notre point de vue, la question de la maîtrise de la personne publique sur le fonctionnement de l'algorithme pose, tout d'abord, la question des algorithmes apprenants, dont les décisions échappent par essence au concepteur de l'algorithme. A cet égard aussi, la décision précitée rendue par le Conseil constitutionnel le 12 juin 2018[330] est très éclairante, ce dernier précisant que « *le responsable du traitement doit s'assurer de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard. Il en résulte que ne peuvent être utilisés, comme fondement exclusif d'une décision administrative individuelle, des algorithmes susceptibles de réviser eux-mêmes les règles qu'ils appliquent, sans le contrôle et la validation du responsable du traitement* ». Il s'agit là d'une garantie essentielle, visant à la préservation des droits des individus mais aussi à la préservation même de notre État de droit et de la légitimité de la puissance publique.

[330] Cons. 71.

Mais la capacité de contrôle de l'algorithme par la personne publique qui le met en œuvre n'est pas seulement susceptible d'être remise en cause par cette éventuelle capacité autoapprenante. N'oublions pas que l'administration a vocation à être cliente d'entreprises qui développent à grands frais des systèmes de détection de comportements anormaux ou d'identification et de suivi biométrique. Ces systèmes, qui ont naturellement vocation à être associés aux drones de sécurité, ne risquent-ils pas de provoquer une forme de délégation illégale des missions de police administrative ?

Si certaines missions de service public peuvent sans difficulté être confiées à des entreprises privées, les exemples historiques sont nombreux en ce sens[331], la question de la délégation de missions dites « régaliennes » pose à cet égard bien plus de difficultés. Le Conseil d'État a rendu sur ce point un avis n° 340.609, qui a été complété par une circulaire du 7 août 1987 relative à la gestion par les collectivités locales de leurs services publics locaux[332]. Cette circulaire est importante car elle implique une limite générale, à savoir que les collectivités territoriales ne peuvent se décharger sur une personne privée de l'exécution des missions qui relèvent de l'exercice même d'une prérogative de puissance publique, notamment l'exercice du pouvoir de police. En matière de contrôle du stationnement payant, il a ainsi été jugé qu'une convention ne pouvait déléguer « *des prérogatives de police du stationnement sur la voie publique confiées par la loi au maire de la commune* »[333]. Il faut donc séparer les activités de pure police administrative de celles annexes, les secondes étant susceptibles de délégation au contraire des premières. Ainsi, dans le cas précité, « *si l'exploitation du stationnement payant souterrain et en surface peut être déléguée, la convention de délégation ne peut prévoir de mettre à la disposition du délégataire les agents municipaux chargés de constater les infractions* »[334]. Cette problématique a récemment connu un regain d'intérêt, avec notamment la question des véhicules radars « mobiles-mobiles » conduits par des opérateurs privés. Appliquée à la question des algorithmes de

[331] V. par exemple la célèbre affaire « Thérond » jugée par le Conseil d'État le 4 mars 1910.
[332] *JO* du 20 décembre 1987, pages 14863 et s.
[333] CE, SSR, 1er avril 1994, n°144152 et n°144241, Commune de Menton, Leb. p. 176 ; *Dr. adm.* novembre 1994, concl. S. LAVISGNES ; *RDP* 1994, p. 1827, note J.-B. AUBY.
[334] P. TERNEYRE, « La notion de convention de délégation : éléments constitutifs et tentative de délimitation sommaire », *AJDA*, 1996, 588.

détection de comportements anormaux associés aux drones de sécurité, cette problématique présente une acuité toute particulière. Ainsi, s'il s'agit simplement pour la puissance publique d'obtenir l'aide matérielle d'une société privée qui va développer sur ses instructions précises et documentées l'algorithme, il n'existe pas de notre point de vue d'obstacle juridique. Mais la réalité du marché est bien différente, et amène certaines entreprises privées à définir elles-mêmes, dans les algorithmes qu'elles développent, les paramètres de ce qu'est un comportement anormal. En pareille situation, même si la décision finale – par exemple l'interpellation d'un individu présenté comme suspect par l'algorithme – relève de la puissance publique, ne doit-on pas considérer que cette décision a été prise sur la base d'un filtrage, peut-être perfectible, qui échappe quant à lui pour sa part largement, voire totalement, à la puissance publique ?

La question est à ce jour largement ouverte mais il nous semble qu'au-delà des mutations éventuelles du droit positif applicable, la question est celle de l'avenir même de la puissance publique, de sa légitimité et donc, par extension de celles de nos institutions.

Conclusion

La sécurité publique, composante essentielle de l'ordre public, bénéficie de moyens évolutifs dont les outils numériques font partie intégrante. Ces derniers offrent de nouvelles capacités, notamment celles de collecter plus massivement des données, d'analyser massivement les agissements des individus, voire de les prédire. Les forces de l'ordre, pour ne pas être dépassées par l'ampleur que prennent les activités criminelles et plus particulièrement terroristes, peuvent être tentées de se reposer sur ces outils dotés de grandes capacités de stockage mais aussi d'analyse des événements et du comportement des individus. Cette facilitation de l'exercice de leur mission peut aussi être considérée comme une forme de délégation de missions régaliennes susceptibles de remettre en cause certaines libertés fondamentales. Plus que jamais, la question de l'acceptabilité juridique et sociale doit être au cœur de la recherche technologique, au risque d'une remise en cause profonde des liens de confiance entre l'État et ses citoyens.

Algorithmes - Données à caractère personnel - Drones - Libertés fondamentales - Ordre public.

Bibliographie sommaire indicative

CHEVALLIER-GOVERS, Constance (Dir.), *L'échange des données dans l'Espace de liberté, de sécurité et de justice de l'Union européenne*, Éditions Mare & Martin, Grenoble, 2017, 559 p.

DE DAVID BEAUREGARD-BERTHIER, Odile et TALEB-KARLSSON, Akila (Dir.), *Protection des données personnelles et Sécurité nationale : Quelles garanties juridiques dans l'utilisation du numérique ?*, Éditions Bruylant, Bruxelles, 2017, 279 p.

GRABIAS, Fanny, « La transparence administrative, un nouveau principe ? », *JCP A.*, n°50, 17 décembre 2018, 2340.

GRANGER, Marc-Antoine, *Constitution et Sécurité Intérieure : Essai de modélisation juridique*, Éditions LGDJ, Paris, 2011, 493 p.

HANICOTTE, Robert, « Une nouvelle catégorie d'OVNI juridique: les drones », n°317, *Gaz. Pal.*, 13 novembre 2014, p. 6.

LAVENUE, Jean-Jacques et VILLALBA, Bruno (dir.), *Vidéo-surveillance et détection automatique des comportements anormaux : Enjeux techniques et politiques*, éd. Septentrion, 2011, 294 p.

SIBER, Jonas, « L'image et le manifestant », n°4, *Gaz. Pal.*, 24 janvier 2017, p. 81.

TERNEYRE, Philippe, « La notion de convention de délégation : éléments constitutifs et tentative de délimitation sommaire », *AJDA*, 1996, 588.

De la transparence comme principe général à l'ère de la plateformisation de l'économie ?

Célia ZOLYNSKI

Professeur de droit privé,
École de Droit de la Sorbonne, IRJS

Karine FAVRO

Maître de conférences de droit public, HDR,
Université de Haute-Alsace, CERDACC

La contribution à suivre est le fruit d'une recherche menée en Master 2 Propriété intellectuelle et droit des affaires numériques (PIDAN) par Mesdames Geneviève Bonhomme et Colombe de Montety, alors étudiantes, qui avaient travaillé dans le cadre de leur mémoire de fin d'année rédigé sous notre direction, respectivement sur la neutralité des algorithmes et sur les discriminations résultant de l'utilisation d'algorithmes.

Traiter de la neutralité des algorithmes, des discriminations, de la transparence ou de leur loyauté, principes régulièrement évoqués en l'espèce, revient à interroger le risque d'appauvrissement des contenus mis à disposition par les opérateurs de plateformes du fait d'une « datapulation » [335] ou encore de rétrécissement de l'accès au marché pour certains acteurs. Cet appauvrissement qu'il soit intellectuel, culturel ou commercial, pose en réalité

[335] C. CASTELLUCCIA, « La « datapulation » ou la manipulation par les données », *La Revue européenne des médias et du numérique*, hiver 2018-2019, n°49, p.92 ; Trois techniques de manipulation des données disséminées par l'internaute sont à dénombrer contribuant ainsi à l'appauvrissement ; celle qui consiste à manipuler l'information, celle qui permet une manipulation psychologique ou cognitive en cherchant à exploiter les faiblesses et biais cognitifs des utilisateurs, et enfin celle dont le but est de tromper l'utilisateur ou le piéger pour le pousser à agir dans un sens déterminé. Cependant, toutes les données ne sont pas disséminées par l'internaute lui-même, mais par d'autres utilisateurs, comme c'est le cas sur les réseaux sociaux. Tout comme il existe des données cachées dans les systèmes informatiques ou des métadonnées qui fournissent des informations précises sur un individu, déduites par exemple d'appels téléphoniques. Réflexion qui se prolonge désormais s'agissant du design : v. sur ce point CNIL, *La forme des choix : données personnelles, design et frictions désirables*, 6e Cahier IP, 2019.

une question essentielle : celle du modèle de société que nous souhaitons promouvoir. Sans remettre en cause la société actuelle par une vision trop idéaliste de ce qu'elle pourrait être, il convient simplement de l'assumer en ayant pleinement conscience de cette manipulation lors de l'exercice de la liberté de choix. L'appauvrissement et la « monopolisation des contenus » doivent être clairement énoncés et assumés par les opérateurs qui y procèdent, à l'image de certaines places de marché. Parallèlement, d'autres opérateurs doivent être en mesure de proposer des contenus plus diversifiés ce qui suppose de réfléchir à la conception algorithmique de cette diversité et à l'application de méta principes juridiques partagés par la communauté scientifique, et la communauté internationale.

Le droit positif : le choix de la loyauté. Par définition, les algorithmes ne sont pas neutres à la fois dans leur conception et dans leurs usages, ce qui signifie que pour en limiter les effets, il convient de construire non pas un droit des algorithmes mais une « *gouvernance des algorithmes* »[336] qui s'entend d'une complémentarité entre des valeurs et comportements éthiques déterminés par les opérateurs et autres acteurs des écosystèmes numériques, et penser les principes juridiques qui encadrent la démarche, comme « *le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques (…) ou affectant l'individu de manière significative* »[337]. Certes, ce dispositif souffre de tempéraments et s'efface devant le consentement de la personne concernée[338]. En réalité, la retranscription de ce droit dans le cadre de la législation française s'est transformée en une simple interdiction de principe « (*témoignant) de ce que le régime des décisions automatisées est loin d'avoir trouvé son point d'équilibre* »[339]. Il est toujours possible pour l'administration de prendre une décision individuelle sur le seul fondement d'un traitement automatisé à condition de respecter les conditions posées par le Conseil constitutionnel[340]. Si le droit des données personnelles intervient à titre principal pour en gérer les usages, et les conséquences sur la vie privée des

[336] L. GODEFROY, « Le code algorithmique au service du droit », *D*. 2018, p.734.
[337] RGPD, art. 22.
[338] V. sur ce dispositif que l'on retrouve à l'article 47 de la loi Informatique et libertés, révisée.
[339] V. sur ce point l'analyse détaillée de J. ROCHFELD, « L'encadrement des décisions prises par algorithme », *Dalloz IT/IP*, 2018, p.474.
[340] Cons. Const. n°2018-765 DC, 12 juin 2018.

individus, cette législation n'est pas suffisante dès lors qu'il s'agit de régir la conception des algorithmes et par conséquent tous les contenus mis à disposition, notamment ceux traitant de données non personnelles[341]. A ce titre, il convient de remonter au rang des principes, et toute la difficulté consiste à y appliquer le principe idoine partagé par toutes les communautés.

L'application du principe de neutralité, initialement prônée par le Conseil national du numérique[342], n'a pas eu les faveurs du législateur français qui a érigé, dans le cadre très circonscrit du droit de la consommation, le principe de loyauté des plateformes lequel sous-tend que les utilisateurs /consommateurs doivent disposer d'informations liées aux types d'algorithmes utilisés par les opérateurs de plateformes dans le cadre des services en ligne marchands mis à disposition[343]. La reconnaissance du principe de loyauté des plateformes répond à une double nécessité. D'une part, celle de reconnaître l'existence des plateformes[344] en les distinguant, certes avec difficultés, des autres prestataires techniques. C'est ce qu'a fait le Conseil d'État dans son rapport annuel dédié au Numérique et droits fondamentaux de 2014[345]. D'autre part, celle de leur appliquer un « succédané » de neutralité afin de prendre en considération les récriminations des éditeurs et hébergeurs qui souffrent de la position dominante des GAFA. Par-delà, c'est l'ensemble des professionnels qui souffre des préférences accordées aux plateformes, en rupture avec les règles classiques du droit de la concurrence. Les professionnels européens ne sont pas en capacité de faire le choix de la diversité, n'ayant pas accès aux données pour y parvenir. Stockées au sein de *data center* outre atlantique ou dans des États qui s'érigent en « paradis des données » poussant aux pratiques de forum shopping, ces données sont trustées et « localisées » pour les besoins d'une poignée d'opérateurs les utilisant au mépris de la transparence. A titre principal, c'est pour cette raison que l'Union européenne a adopté au mois de novembre dernier un Règlement visant à la libre circulation des données non

[341] V. en ce sens, CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'Intelligence artificielle*, rapport déc. 2017, spéc. p. 46 et s.

[342] CNNum, *Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouvert et soutenable*, mai 2014.

[343] C. ZOLYNSKI, « Loyauté des plateformes : de la réglementation à la multirégulation », *Cah. Droit entr.* 2017, étude 16.

[344] Appellation qui avait d'ailleurs été adoptée par N. COLIN et H. VERDIER, *L'âge de la multitude*, *Entreprendre et gouverner après la révolution numérique*, Armand Colin, 2014.

[345] CE, *Le numérique et les droits fondamentaux*, Étude annuelle, Doc. Franç., 2014, p.273.

personnelles et interdisant leur « localisation » au bénéfice d'un État ou d'une poignée d'opérateurs[346].

En réalité, le débat n'est pas tranché. Pour autant, le principe de loyauté paraît désormais irriguer l'ensemble des activités des plateformes. Mu en principe général d'un « droit des plateformes » en construction, il s'appliquerait de façon transversale, quoi que sous des formes distinctes, adaptées aux contenus ou relations saisies par la réglementation[347]. Le droit de l'Union européenne paraît ainsi l'étendre à la sphère commerciale avec l'adoption du règlement « Platforms to business » (dit « P to B »)[348], même si le terme n'est pas présent dans la nouvelle réglementation. Le principe de loyauté dérive alors des principes de transparence et d'équité, plus largement partagés par l'ensemble des États membres, qui imposent aux plateformes d'informer leurs utilisateurs professionnels sur leurs intentions notamment quant aux produits distribués et aux données collectées.

S'agissant du droit interne, on trouve désormais trace du principe de transparence au sein de la proposition de loi de Madame Avia, visant à lutter contre la haine sur Internet et les lois n°2018-1202 et n°2018-1201 du 22 décembre 2018 relative à la manipulation de l'information, dites lois *Infox* en lien avec la transparence des publicités politiques et des algorithmes. Appliquée aux contenus purement informatifs truffés de discours haineux, de « fausses nouvelles et de nouvelles fausses »[349], la loyauté s'inscrirait dans le prolongement de l'honnêteté de l'information, véritable impératif déontologique qui n'a pas sa place en tant que tel dans les rapports commerciaux au risque de porter atteinte à la liberté d'entreprendre.

En somme, la loyauté s'érigerait en la forme d'un principe matriciel mis en œuvre soit dans le cadre de relations contractuelles, soit dans le cadre de codes de bonne conduite produits par les acteurs concernés, d'une éthique des algorithmes, etc., nécessaires à la régulation des plateformes.

[346] Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne.
[347] C. ZOLYNSKI, « Infox : quelle régulation à l'ère de la société de la désinformation ? », SLC, Tribodien, 20 janvier 2019, à paraître.
[348] Proposition de Règlement du Parlement européen et du Conseil promouvant l'équité et la transparence pour les entreprises utilisatrices des services d'intermédiation en ligne COM/2018/238 final.
[349] Expression utilisée par A.-E. DE CRÉVILLE, *Légipresse,* n°364, octobre 2018, p.467.

L'intérêt d'une consécration de la neutralité. La loyauté et la neutralité sont deux principes inhérents à l'écosystème numérique et constituent, par essence, les fondements d'un droit de la régulation des communications numériques[350]. D'une part, ils incarnent l'évolution des principes directeurs du droit de la communication, guidée par la nécessité de s'adapter à ce nouvel environnement. Le principe de pluralisme des idées et des opinions, garanti dans le domaine de la communication audiovisuelle, s'applique difficilement aux acteurs du net au regard de la bulle algorithmique dans laquelle est enfermé progressivement l'utilisateur en réduisant sa liberté de choix du fait d'une hyper personnalisation des contenus qui amplifie les biais sociologiques et cognitifs. C'est au regard de l'homophilie et du biais de confirmation que l'utilisateur va s'identifier auprès d'individus miroir de lui-même ce qui ne pousse ni à la diversité des contenus, ni même à leur pluralité[351]. Si l'on admet que les services en ligne sont avant tout des services d'information, le pluralisme doit y avoir sa place, mais dans une approche rénovée qui mêle les aspects techniques aux contenus. Dans cette perspective, c'est alors la neutralité qui s'impose, contribuant à « objectiviser » l'approche de la diversité et à protéger les opérateurs les moins puissants du marché de la poignée de GAFA qui règne en maître du système qu'ils ont créé et justifiant la promotion d'une régulation *ex ante* et asymétrique[352]. Certes, l'application du principe de neutralité ne permet pas de garantir la neutralité de l'algorithme ou la logique ouverte des plateformes, mais au même titre que le principe de pluralisme ne permet pas d'imposer la diversité mais seulement la pluralité des contenus, à tout le moins dans sa dimension nationale. Par ailleurs, l'application stricte du principe de neutralité aux algorithmes aurait un effet contreproductif en appauvrissant davantage les contenus mis à disposition des internautes excluant les big data.

Ce n'est pas de cette approche réductrice de la neutralité dont il convient de se saisir mais plutôt d'aborder le sujet sous l'angle de la « neutralité des contenus », par exemple pour préserver le débat démocratique en imposant aux plateformes la diffusion de nouvelles « neutres » - comme les dépêches des

[350] K. FAVRO, *Le droit de la régulation des communications numériques*, LGDJ, Systèmes, novembre 2018.
[351] C. ZOLYNSKI, *loc.cit.*
[352] V. Consultation organisée par le Conseil national du numérique dans le cadre des états généraux des nouvelles régulations numériques, https://egnum.cnnumerique.fr ; v. également, K. FAVRO, *Communications numériques – Régulation et résolution des litiges*, LGDJ, Systèmes, avril 2019.

agences de presse - ou de pousser des contenus en fonction de paramètres distincts de ceux commandés par leurs seuls intérêts économiques. Autrement dit, il s'agit de restaurer le pluralisme à l'aide d'une nouvelle logique algorithmique et de données d'entrées afin d'assurer la diversité des contenus. L'objectif serait alors d'entendre la majorité silencieuse, ce que garantit par ailleurs le principe de pluralisme des idées et des opinions tel qu'il est consacré par le droit français, en ce qu'il donne la prime à la majorité dans le cadre d'une approche purement quantitative[353].

En actant du principe de neutralité, ce qui est visé c'est l'« effet cliquet » qui impose au législateur de garantir la neutralité sans « retour-arrière », et à l'autorité de régulation compétente, de garantir l'application du principe à l'égard des opérateurs de plateforme et de l'ensemble des acteurs. En l'état, il appartiendrait donc à l'ARCEP de s'ériger en garant de la neutralité par la mise en œuvre d'un pouvoir de régulation plus abouti qu'il ne l'est actuellement. Il est en effet souhaitable de privilégier une approche souple et pragmatique pour ne pas faire obstacle à l'innovation et la qualité des services proposés. C'est tout le paradoxe. Les opérateurs sont favorables à la régulation procédant de la rédaction d'un code de bonne pratique qui comporterait une forme de « supervision » collaborative, et des sanctions pour ceux qui ne respecteraient pas leurs engagements[354]. Rien de nouveau en réalité, si ce n'est la volonté d'y parvenir en transformant le jeu des acteurs.

L'émergence « d'un » principe de transparence. Les notions de neutralité et de loyauté ont en commun l'idée de transparence. Alors que la neutralité demeure le corollaire du principe d'égalité, la loyauté procède d'une subjectivisation de la transparence résultant de l'accès et de la garantie d'un droit à l'information. La loyauté, entendue comme la transparence, s'écarte irréversiblement des mécanismes répressifs du droit de la presse, pour régir *a priori* le comportement des opérateurs (moteurs de recherches, réseaux sociaux, *marketplaces*, comparateurs de prix, etc.) à l'égard des consommateurs, mais pas seulement, car la loyauté doit s'appliquer à tout type de contenus et protéger les professionnels ou plus globalement les internautes.

[353] V. C. ZOLYNSKI, *loc.cit.*; K. FAVRO, Droit de la régulation des communications numériques, préc.
[354] Avis du CNNum n°2013-1 et rapport n°2013-1 du 1er mars 2013 sur la neutralité.

La finalité de ce principe repose sur la confiance de l'utilisateur/consommateur dans l'économie numérique, véritable moteur de cet écosystème[355].

Des liens sont désormais à construire entre la transparence et la mise en œuvre d'une diversité. Autrement dit, la transparence doit se penser comme un mécanisme d'incitation à la diversité. Cette incitation a pu être directe s'agissant de l'application du principe de pluralisme aux anciens modèles de communication (presse et audiovisuel)[356]. Probablement qu'elle se construira de manière plus indirecte par une information permettant de comparer les offres commerciales et de contenus dès lors que, désormais, la transparence vise également à restaurer la liberté de choix du consommateur/internaute dans une logique d'empowerment, afin de préserver ses libertés individuelles ainsi que le débat démocratique.

Le principe de transparence permet, certes, de poser des règles dès la conception de l'interface de la plateforme pour intégrer des valeurs et des objectifs à atteindre, même dans l'analyse des algorithmes, mais ne doit pas se limiter à un simple devoir d'information sans contrepartie[357]. Partant, et dans la mesure où la question de la régulation des algorithmes est traitée pour davantage de réalisme dans un cadre européen, c'est l'esprit de ces principes qui doit y être retranscrit quelle que soit la dénomination choisie... Le principe de transparence, qui transcende les divisions les plus classiques du droit et des communautés scientifiques, doit se reconstruire à l'aune de ces nouveaux enjeux, pour asseoir le modèle de société de demain !

[355] V. la Proposition de Règlement du Parlement européen et du Conseil promouvant l'équité et la transparence pour les entreprises utilisatrices des services d'intermédiation en ligne, préc.
[356] P. MARCANGELO-LEOS, *Pluralisme et audiovisuel*, LGDJ, Bibliothèque de droit public, t. 240, 2004.
[357] C. consom., art. L.111-7.

L'encadrement juridique de la prédiction

Geneviève BONHOMME et Colombe DE MONTETY

Juristes PI-Numérique

Longtemps l'homme a poursuivi une perpétuelle quête de l'avenir. Dans cette recherche de la connaissance du futur, l'homme a fait preuve au cours des temps d'une créativité débordante. Entre oracles et augures, entre divination et expérimentation, pléthore de méthodes ont été inventées pour y parvenir. Très tôt, l'anticipation de l'avenir s'est scindée en une double catégorie reposant sur l'existence ou non d'une méthode scientifique. Cette dichotomie s'est également retrouvée dans la terminologie employée pour les méthodes en question. Ainsi, à la prédiction sont laissées les méthodes divinatoires proclamant l'avenir en opposition à la prévision qui s'attache aux méthodes davantage fondées sur un raisonnement scientifique. Paradoxalement, si les méthodes de prévision ont pris le pas sur celles de prédiction au fil des siècles, la confiance en celles-ci s'est développée de manière inversement proportionnelle[358]. Le perfectionnement des méthodes de prévision a récemment connu un sursaut considérable avec l'expansion des algorithmes.

En matière algorithmique, plusieurs familles se distinguent en vertu d'un critère finaliste. Il existe notamment les algorithmes probabilistes et déterministes[359], les algorithmes dits prédictifs[360], les algorithmes récursifs[361],

[358] A titre d'exemple, les prédictions de la pythie de Delphes constituaient une véritable institution respectées de l'ensemble du peuple grec. *A contrario*, il est aujourd'hui possible de constater une importante vague de défiance à l'encontre des algorithmes prédictifs. Voir par exemple P. SIRINELLI, S. PREVOST, « Madame Irma, magistrat », *Dalloz IP/IT*, 2017, p. 557

[359] Rapport CNIL, *Comment permettre à l'Homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, décembre 2017, p. 18 : Les algorithmes déterministes sont ceux dont les critères de fonctionnement sont explicitement définis par ceux qui les mettent en œuvre et les algorithmes probabilistes sont ceux qui reposent sur un mode d'apprentissage type *deep learning* ou *machine learning*.

[360] Ces algorithmes prédictifs sont notamment utilisés dans le domaine de la police et de la justice. Voir F. DEFFERRARD, C. PAPINEAU, « Le pouvoir de jurisdictio des algorithmes aux États-Unis : entre fantasme et réalité jurisprudentielle », *Dalloz IP/IT*, 2017, p. 668.

les algorithmes itératifs[362]. Parmi cette diversité, les algorithmes de prédiction perpétuent cette traditionnelle quête de la connaissance de l'avenir. Qu'il s'agisse de forêts aléatoires ou de réseaux de neurones, ce sont des mécanismes de calcul de probabilité en fonction de critères prédéfinis et d'une base de données. Malgré le raisonnement scientifique sur lequel se fonde ces algorithmes, la terminologie employée[363] traduit le manque de confiance à l'égard de ces méthodes de prévision. Cette méfiance est particulièrement étonnante dans la mesure où ces algorithmes prédictifs peuvent intervenir dans des domaines régaliens tels que la justice ou la police. Ces terrains d'expansion peuvent concerner des questions de sécurité, d'ordre public. Les enjeux sont aussi importants que les risques d'une telle utilisation peuvent l'être, d'autant plus qu'ils ont quitté leur stade expérimental pour passer à la prédiction d'événements, de comportements qui sont directement à même d'être interprétés par les scientifiques et spécialistes des différents secteurs[364].

Eu égard à l'importance des champs d'intervention des algorithmes prédictifs, ils doivent faire l'objet d'un encadrement juridique précis. L'objectif d'un tel cadre vise à éviter la survenance de biais algorithmiques, c'est-à-dire que l'algorithme donne un résultat éloigné d'une norme de référence. Ce n'est pas tant la nécessité d'un principe pour encadrer le fonctionnement des algorithmes que le choix du principe qui aujourd'hui n'obtient pas consensus. La tâche est d'autant plus délicate que l'objet du principe n'a pas encore révélé son complet potentiel, ni les risques qui l'accompagnent. Leur complexité et les utilisations multiples dont ils sont amenés à être les sujets ne permettent pas à ce jour de dresser une liste exhaustive des biais qu'ils présentent. Ce constat posé, le choix du principe ne doit pas y être étranger. Un principe dont la définition et la portée seraient trop étroites ne pourrait pas saisir l'ensemble des risques. Sa rigidité, confrontée à un instrument dont l'évolution et l'étendue est exponentielle, le précipiterait dans la désuétude. De plus, la

[361] L'algorithme fait appel à lui-même dans son code. Cela signifie qu'il exécute sa tâche en répétant n fois le protocole fixé. Pour une meilleure visualisation de l'algorithme récursif, voir les fractales qui sont des figures produites à partir d'un mécanisme similaire.

[362] L'algorithme part d'une entrée de départ et va essayer sur celle-ci plusieurs itérations qui vont fournir des ébauches de solution. Chaque itération aura vocation à préciser ces ébauches successives afin d'arriver à une solution satisfaisante.

[363] On parle de prédiction algorithmique et non pas de prévision algorithmique.

[364] Il s'agit par exemple du logiciel d'Anacrim. Pour plus d'informations voir H. GUILLAUD, "Police prédictive (½) : dépasser la prédiction des banalités", *Le Monde*, 24 septembre 2017.

prédiction est un exercice délicat dont la vérification est toujours complexe. En revanche, si ce principe doit présenter une certaine souplesse d'utilisation, il doit pour autant faire l'objet d'une définition précise dans le droit positif afin qu'il puisse avoir une portée effective et être opposable par le justiciable en cas de litige.

Une réflexion doit ainsi être menée pour esquisser le principe le plus à même de fournir une protection aux justiciables. Dans un souci d'effectivité, le principe doit accompagner l'élaboration de la prédiction pour prévenir les risques intrinsèquement liés à ce processus. Toutefois, il convient d'éviter le travers consistant à envisager d'emblée la transposition ou la création d'un principe, taillé sur mesure, aux risques de la prédiction. Une étude des principes juridiques existants s'avère alors opportune **(I)** avant d'envisager ensuite de se tourner vers un principe novateur **(II)**.

I) Le recours inefficace aux principes traditionnels pour encadrer les prédictions

La réflexion et la construction de l'arsenal législatif encadrant la prédiction se sont réalisées en écho des risques qu'un tel emploi des algorithmes laissait apparaître.

Les traitements algorithmiques à des fins prédictives sont venus placer un voile opaque sur l'utilisation des données, les opérations dont elles font l'objet et leurs finalités. En réponse à cette obscurité, la stratégie législative repose sur l'information des individus. Elle se traduit par la combinaison de deux principes : la loyauté et la transparence **(A)**. L'objectif de ces principes est l'apport d'une connaissance relative à leur utilisation. C'est en ce sens que le principe de transparence a évolué permettant de délivrer une information concernant l'existence et l'utilisation d'algorithmes prédictifs. Cette obligation est consolidée par le principe de loyauté, permettant d'exiger une fiabilité des informations transmises. Ces principes composent actuellement l'arsenal de protection face aux risques de la prédiction. Toutefois, il apparaît que la seule connaissance quant à l'utilisation de traitements algorithmiques est apparue insuffisante. Afin de la consolider, le dessein du législateur consiste à porter la protection sur les effets de ces traitements et des moyens de protection

pouvant être déployés à leur encontre. Des principes plus traditionnels ont été évoqués pour contrecarrer ces effets : l'égalité et la non-discrimination **(B)**. Leur proximité dans leur essence propre en fait toutefois des principes aux effets distincts dans la sphère algorithmique. L'opportunité d'un principe d'égalité et de non-discrimination pour l'encadrement des algorithmes reste à confirmer. En effet, bien qu'envisagés pour limiter les dérives de la prédiction, ils laissent transparaître des faiblesses intrinsèques à l'encadrement des risques possibles en matière de prédiction.

A) Les principes de transparence et de loyauté

Bien que profondément liées, la transparence **(1)** et la loyauté **(2)** se distinguent pourtant par des dispositifs juridiques différents.

1) La transparence

Le principe de transparence est un concept répandu en droit français comme européen (processus électoraux, accès aux documents administratifs…[365]), tout en étant sujet à des limites (secret d'Etat, protection de la vie privée, secret des affaires[366]). Elle se comprend comme un moyen d'obliger à rendre des comptes. Cette notion objective se traduit en une obligation pour l'acteur de communiquer sur les opérations menées concernant les personnes. Puisque le traitement de données est bien souvent invisible, l'idée paraît indispensable et légitime.

En droit de la consommation, les opérateurs de plateformes en ligne doivent énoncer les critères de référencement utilisés pour le classement des résultats d'une recherche[367] ; la finalité ici est d'informer les utilisateurs ainsi que de lutter contre la concurrence déloyale qui est pratiquée à partir des critères.

[365] Définition de la transparence, Lexique des termes juridiques, 20ème édition, Dalloz, p.903.
[366] Idem.
[367] C. consom., art. L.121-1 à L.121-7.

Le Règlement général de protection des données (RGPD)[368] défend une vision large de la transparence[369], principe fondamental de tout traitement de données personnelles. Elle ne consiste pas seulement en la fourniture de détails sur le traitement lui-même, mais également sur son existence[370], ses risques[371]. La loi française[372] va plus loin dans les informations à communiquer (sur demande de la personne), quand une décision administrative est automatisée[373]. Sur ce fondement, le Tribunal administratif de Guadeloupe a récemment enjoint au président de l'université des Antilles la communication des procédés algorithmiques et du code source relatif au traitement des candidatures d'entrée en licence sur la plateforme Parcoursup[374]. Le fort enjeu de cette plateforme justifie de donner aux candidats les clés pour comprendre le fonctionnement de l'outil d'aide à la décision.

Il apparaît bien que la transparence est inéluctable pour la confiance et l'acceptation des traitements algorithmiques par tous. Concrètement, la transparence entraîne la communication d'informations à propos du traitement mis en oeuvre[375] (pour un profilage, des éléments supplémentaires sont requis[376]). Selon Marie Mercat-Bruns[377], la logique intrinsèque du droit de non-discrimination est une incitation à la transparence sur les mécanismes et règles, par les personnes en situation de pouvoir. Mais leur communication est insuffisante, pour deux raisons. En premier lieu, une prédiction s'appuyant sur des critères discriminants ne peut être résolue par la transparence, tant l'identification de critères discriminants est malaisée : lire entre les lignes des

[368] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[369] RGPD, art. 5 a).
[370] RGPD, considérant 58 : « la personne concernée soit informée de l'existence de l'opération de traitement et de ses finalités ».
[371] RGPD, considérant 39 : « Les personnes physiques devraient être informées des risques, règles, garanties et droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement ».
[372] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.
[373] CRPA, art. L.311-3-1.
[374] TA Guadeloupe, 4 février 2019, n°1801094.
[375] v. par exemple les listes des articles 13 et 14 du RGPD.
[376] Art. 13 f) : « l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ».
[377] M. MERCAT-BRUNS, «Le droit de la non-discrimination, une nouvelle discipline en droit privé ? », *D.*, 2 févr. 2017, p.224.

critères de raisonnement n'est pas à la portée de tous ; tandis que des critères en apparence "neutres" pourraient se révéler biaisés[378]. Encore plus, le machine learning bouscule cette idée en modifiant à chaque itération le raisonnement de la machine[379].

Dans un second temps, la transparence est insuffisante en ce qu'elle n'assure pas une compréhension de l'information par les individus : c'est la critique adressée par la CNIL[380] : elle plaide pour l'intelligibilité de l'information. A cette fin, la transparence doit s'accompagner d'une loyauté de l'information communiquée.

2) La loyauté

Le droit français connaît, d'abord, une application particulière de la loyauté en droit de la consommation. La loyauté renvoie à une conformité de l'action du professionnel aux usages du commerce. Le lourd arsenal juridique[381] sanctionnant les différents types de pratiques commerciales déloyales atteste de l'importance de cette loyauté dans les relations entre les professionnels et les consommateurs. La transparence, la prévisibilité et plus encore l'équité de traitement, acquièrent une place de choix en Europe, cette fois dans les relations entre professionnels et plateformes en ligne (y compris moteurs de recherche)[382]. Dans ce projet de règlement inspiré par celui du Code de la consommation, les plateformes doivent fournir des explications sur leurs décisions et activités, ce qui en permet un certain contrôle par les entreprises utilisatrices.

Définir la loyauté n'est cependant pas aisé ; ce peut être une honnêteté, bonne foi (« assurer de bonne foi le service de classement ou de

[378] Par exemple, la décision du Défenseur des droits du 18 janvier 2019 n°2019-021 relative au fonctionnement de la plateforme nationale de préinscription en première année de l'enseignement supérieur (Parcoursup), soulève la possibilité pour le critère du "lycée d'origine" d'être une pratique discriminatoire, s'il aboutit à exclure des candidats sur la plateforme.

[379] Dans cette situation, une autre idée à défendre peut être la traçabilité des systèmes apprenants : v. J.-M. DELTORN, « La protection des données personnelles face aux algorithmes prédictifs », *RDLF* 2017, chron. n°12 (Revue droits et libertés fondamentaux).

[380] Rapport CNIL, Comment permettre à l'Homme de garder la main ?, op.cit. p.51.

[381] C. consom., art. L.121-1 à L.121-7

[382] Voir à ce sujet la proposition de règlement européen « promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne », 26 avr. 2018.

référencement »[383]). Dans ce cas, elle a un sens objectif, qui s'intéresse au fait de savoir si le service proposé correspond au service réellement délivré, par exemple. Cette acception s'attache à la démarche de l'acteur (transmettre une information). Mais la loyauté peut avoir un sens subjectif, imposant à un acteur qu'il serve les intérêts des utilisateurs ou consommateurs, et non pas les siens. La loyauté se rapproche alors de l'éthique, de la finalité recherchée par l'acteur, qui doit être "bonne". Ici, le danger est que chaque acteur adopte sa propre conception de la loyauté et de l'éthique.

Les droits français et européen consacrent enfin la loyauté des algorithmes comme un principe fort. La loi pour une République numérique[384] impose une loyauté pour les opérateurs de plateformes, via une obligation d'information[385]. La loyauté est alors encore une transparence, entre professionnel et consommateur. De plus, elle tient aussi une place indispensable en droit des données personnelles, place réaffirmée par le Règlement général de protection des données[386]. Principe directeur de tout traitement de données personnelles[387], la loyauté ne repose néanmoins sur aucune définition précise, ce qui ne fait que brouiller le champ précis de ce principe pourtant fondamental. Ainsi, le droit positif a une appréhension étroite et mouvante du principe de loyauté et de ses implications. La flexibilité du principe ajoute en réalité un second niveau de complexité face à un algorithme prédictif, risquant un rejet de ce principe par les acteurs concernés.

Concrètement, dans son premier sens, la loyauté d'un algorithme de prédiction lui imposerait de fonctionner comme il est censé fonctionner. Cette obligation objective de conformer le service apporté au service annoncé peut s'illustrer en s'assurant, en amont, que l'algorithme ne puisse pas dévier son raisonnement vers des résultats faux. Cet aspect peut être encore complété par une obligation de vigilance du responsable de l'algorithme, tout au long de son fonctionnement, pour s'assurer de l'absence de dérives pendant son cycle de « vie ». C'est une idée défendue par la CNIL, lorsque les sciences et connaissances techniques ne peuvent apporter de réponses certaines. Ici, la

[383] CE, *Le numérique et les droits fondamentaux*, Etude annuelle, 2014, p.26.
[384] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique dite loi Lemaire.
[385] C. consom., art. L.111-7 et L.117-1-2 (obligations particulières relatives aux avis en ligne).
[386] RGPD, op.cit.
[387] RGPD, art. 5 §1 (a),

loyauté et la vigilance ont vocation à embrasser tous les cas de figure, que les biais proviennent des paramètres de l'outil ou des données traitées.

Dans sa seconde acception, un algorithme loyal serait un outil au service de ses destinataires, opérant une balance des intérêts, entre ceux des utilisateurs et ceux de l'acteur responsable du traitement. En ce sens, la CNIL estime que la loyauté doit s'appliquer à certains grands intérêts collectifs afin de ne pas créer ou renforcer de discriminations[388]. En effet, la prédiction algorithmique est un moyen de « *connaître les individus afin de mieux les servir, mais aussi de jouer sur leurs sensibilités et d'anticiper leurs réactions* »[389]. Ici, la loyauté conduirait à sanctionner une finalité déloyale du traitement de données, mais ne s'intéresse pas à la manière dont est mené ce traitement. Cette acception de la loyauté est reprise par le juge, ultime interprète du principe, lorsqu'une collecte ou un traitement est suspecté(e) d'être déloyal(e)[390]. Néanmoins, puisque cette notion de loyauté est malléable/subjective, il est difficile d'en dresser les contours nets et fixes pour en saisir les implications pratiques. Si sa flexibilité peut embrasser nombre de conséquences pour les acteurs, si différents soient-ils (secteur, taille, modèle d'affaires), elle ne peut qu'en accentuer l'illisibilité et l'insécurité juridiques en restant peu ou pas définie.

Face à ce constat, la loyauté ne semble donc pas constituer un principe juridique suffisamment stable et net pour réguler efficacement les prédictions algorithmiques. Les différents aspects de ce principe ne sont pas suffisants, et pourraient être inscrits dans un principe plus général, dépassant la simple conception subjective de loyauté. Il s'agit alors de penser un principe plus objectif, d'où découlerait certaines obligations effectives pour les acteurs, touchant directement aux risques de biais dans ces traitements. Puisque la prédiction entraîne une différenciation entre les individus, le principe d'égalité pourrait être mobilisé pour en cantonner les effets.

B) Le principe d'égalité et le principe de non-discrimination

[388] Rapport CNIL*, op.cit*., p.49.

[389] F. PELLEGRINI, « Intelligence artificielle, mégadonnées et gouvernance », *Revue Lamy Droit de l'Immatériel*, n°144, p.56-59.

[390] Pour une collecte loyale : Cass. soc. 13 juin 2018, n°16-25.301, Comm. Y. BASIRE, J. SABBAH, Rev. Trav. 2018. p.680. Pour une collecte déloyale : CE 9 nov. 2015, *Sté Néressis*, n° 384673, Lebon, Comm. *RJDA* n°5, p.410 ; Cass. crim. 14 mars 2006, n°05-83.423, bull., JurisData n°2006-032892, Comm. A. LEPAGE, CCE, n°9, p.43-45.

Parfois utilisés comme synonyme, le principe d'égalité **(1)** et le principe de non-discrimination **(2)** voient leur finalité diverger dans la sphère algorithmique.

1) Le principe d'égalité et la prédiction

Au sein de l'éventail de principes possibles, l'égalité doit être sans conteste étudiée. Principe pilier de la République française[391], a-t-il une légitimité dans la sphère algorithmique ? L'égalité est définie en son versant positif comme le principe selon lequel toute personne doit être traitée de la même façon[392]. En son versant négatif, cela signifie qu'aucun privilège ne peut être accordé à un individu. Sa place en droits français et international n'est plus à démontrer. Chaque pan du droit est imprégné de ce principe. À titre d'exemple, il convient de citer la possible sanction pour rupture d'égalité devant les charges publiques admise en droit administratif[393] ou encore la répartition de la réserve héréditaire en droit des successions[394].

Ce principe républicain imprègne notre société ce qui en fait un parfait prétendant à l'encadrement de la prédiction. Certains considèrent que tout algorithme devrait respecter les lois d'Asimov comme base de tout traitement[395]. La question d'un principe d'égalité régissant le code n'apparaît pas vide de sens tant l'importance de ce principe est omniprésent dans les rapports entre les individus, mais également avec l'administration. « *Traiter tous les individus de façon égalitaire* » pourrait être la ligne de conduite demandée aux algorithmes. Ce principe pourrait, au premier abord, être perçu comme un garde-fou. Les traitements algorithmiques prédictifs ont pour but de prévoir en amont des situations futures. À titre d'exemple, les assurances peuvent sur des données de santé de leurs clients prédire leur état de santé. En fonction de ce résultat, le montant dû pourra être plus élevé pour une personne ayant un état de santé futur moins prometteur et susceptible de plus

[391] Article premier de la Constitution du 4 octobre 1958. Préambule de la Constitution du 27 octobre 1946. Protocole n°12 de la CEDH.
[392] G. CORNU, Vocabulaire juridique, op.cit.
[393] CE, sect., 14 oct. 2011, *Mme Saleh*, req. N° 329788.
[394] C. civ., art. 912.
[395] F. SANGARE, « Pour s'assurer de la loyauté des algorithmes, il faudrait coder les lois d'Asimov et les figer », *Revue Lamy Droit civil*, 2017, p. 36.

de maladies. Le principe d'égalité pourrait être une barrière à de tels comportements, d'autant plus que ces états prédictifs, sur lesquels ils s'appuient, peuvent s'avérer erronés. Ce principe peut revêtir un aspect protecteur contre une utilisation similaire. À la différence de la non-discrimination qui repose sur des critères précis, l'égalité ne serait pas astreinte à ce carcan pour sanctionner de telles utilisations. La liberté d'appréciation apparait opportune face à la complexité de la prédiction.

Bien qu'elle semble protectrice, la question de son adéquation à la sphère algorithmique reste en suspens. Pour cela il faut s'intéresser au fonctionnement des algorithmes. Trois points méritent d'être étudiés. Afin d'obtenir une prédiction cohérente et fiable, la base de données doit être conséquente et variée se rapprochant du mieux possible de la réalité. Dans l'hypothèse où un principe d'égalité serait retenu, les données devraient s'y conformer. En cela, les données constituent les deux premiers points à étudier.

Le premier point porte sur les données traitées par les algorithmes. Elles constituent la matière première à leur fonctionnement. Les algorithmes prédictifs s'appuient sur des situations passées. De ces modèles, ils déterminent la possibilité qu'un événement survienne. Les prédictions s'appuient sur des données dont le nombre et la variété vont avoir un impact direct sur la cohérence et la fiabilité du résultat. La base de données doit être conséquente pour encadrer le maximum de possibilités. Toutefois, le panel de données est dépendant des faits antérieurs. Leur survenance ne répond pas à une logique d'égalité. Par conséquent, il serait possible de constater une inégalité de données par rapport aux zones géographiques alimentant les algorithmes. Appliquer un principe d'égalité sur le panel de données, directement dépendant d'événements indépendants de la conduite humaine, serait inapplicable.

Le second point, quant au fonctionnement des algorithmes, concerne la pondération des données. En effet, ce mécanisme permet de conférer à une donnée sa valeur au sein d'un processus de traitement, d'affecter un poids à une variable. Les données ne se voient pas reconnaître la même importance au sein d'un traitement. La pondération permet d'obtenir un résultat plus fiable et

moins empreint de biais[396]. Un principe d'égalité opposé à la disparité naturelle de la pondération ne serait pas opportun pour la performance des algorithmes.

Quant au dernier point, il est opportun de se questionner sur l'application du principe d'égalité au résultat. Il faudrait toutefois considérer que chaque individu bénéficie d'une égalité des chances dans la détection des événements. Par exemple, si l'algorithme a pour compétence la détection en amont des risques d'incendie au sein d'un secteur, le principe d'égalité pourrait imposer une exigence quant à la performance de prédiction. Cette obligation viendrait directement se confronter à la qualité de la base de données et à l'exhaustivité des situations pour permettre une détection plus fiable, ce qui n'est pas un élément dépendant de l'agent humain. Les algorithmes prédictifs retranscrivent les inégalités préexistantes s'il y en a, même lorsqu'elles sont sous-jacentes[397]. Demander l'égalité au sein des données en écartant celles laissant transparaître une violation du principe serait contre-productif pour la fiabilité du résultat.

Le principe d'égalité pourrait avoir vocation à s'appliquer sur le résultat et son utilisation. Toutefois, le brandir comme celui devant encadrer la prédiction ne serait pas opportun en raison de son faible spectre d'application.

2) Le principe de non-discrimination

L'interdiction des discriminations est une pierre importante de l'édifice du droit français. En effet, elle imprègne chaque pan du droit par une interdiction (pénale) de discriminer en se fondant sur des critères considérés comme interdits[398]. Le texte pénal énumère les critères illégaux sur lesquels une discrimination peut être qualifiée[399]. De surcroît, certains domaines juridiques disposent de leur propre texte interdisant les pratiques discriminatoires (droit

[396] Une seule décision peut impacter le résultat final en raison de l'impact des extrêmes sur les moyennes. E. MARIGUE, « Gouverner par la loi ou les algorithmes : de la norme générale du comportement au guidage rapproché des candidats », *Dalloz IP/IT*, 2017, p. 517.

[397] Voir l'enquête de Propublica du 23 mai 2016 précitée sur la répartition des faux positifs et des faux négatifs par l'algorithme COMPAS en fonction de la couleur de peau des populations concernées.

[398] G. CORNU, *op.cit*.: « une différenciation contraire au principe de l'égalité civile consistant à rompre celle-ci au détriment de certaines personnes physiques […] ou au détriment de certaines personnes morales ».

[399] C. pén. art. 225-1 : origine, sexe, situation de famille, apparence physique, lieu de résidence, état de santé, etc.

social[400], droit des assurances[401]…). Le principe de non-discrimination découle alors du principe d'égalité, et en permet le respect, en interdisant de prendre en compte certains aspects individuels : toute personne privée ou publique est alors tenue à une obligation d'indifférence, lorsqu'elle prend une décision envers un individu, fondée sur un critère constituant sa personnalité.

Ce droit fondamental d'être traité sans discrimination est reconnu par de nombreux textes juridiques[402]. La discrimination est donc un sujet fortement traité au niveau international comme européen et national. Cependant, la spécificité du droit français apporte une complexité particulière à cet objet. Si l'éclatement des textes applicables à la discrimination est le signe de son aspect transversal et fondamental en droit, il en dessert son application concrète qui s'avère complexe.

Il est intéressant de se demander si le principe de non-discrimination peut être un outil efficace pour encadrer une prédiction produite par un algorithme. En effet, une prédiction peut engendrer une décision discriminante envers un individu. Ainsi une prédiction qui s'appuie sur des éléments relevant des opinions politiques d'un individu, peut s'avérer illégale ; il en est de même pour tout autre critère illégal consacré par le Code pénal.

Deux sources de discrimination peuvent être soulevées s'agissant du traitement algorithmique : celle-ci peut résulter de paramètres utilisés dans le raisonnement dès lors qu'ils ne sont pas objectifs (et qui se rapprochent donc de critères illégaux) ; elle peut résulter de la qualité des données qui sont traitées. Certains algorithmes peuvent, en effet, être considérés comme « objectifs » dans leurs critères mais produisant néanmoins des résultats discriminatoires. Ces deux sources de biais engendrent une complexité pour qualifier une discrimination : les paramètres de l'outil ne se rapprochent généralement pas d'un critère illégal, mais conduiront néanmoins à une décision discriminante. De plus, l'algorithme auto-apprenant soulève une difficulté supplémentaire, car ici, l'outil crée ses propres critères de

[400] C. trav., art. 1132-1.

[401] C. ass., art. 133-1.

[402] La Convention internationale de l'Organisation des Nations Unies sur l'élimination de toutes les formes de discrimination raciale de 1966, la Déclaration universelle des droits de l'Homme de 1948 (article 7); le Pacte international des droits civils et politiques de 1966 (article 26) ; la Convention européenne de sauvegarde des droits de l'Homme et des libertés de 1950 (article 14) ; la Charte des droits fondamentaux de l'Union européenne de 2000 (article 21).

raisonnement, rendant leur visibilité et leur maîtrise encore plus ardues. La seconde source de discrimination, les données biaisées ou fausses, appelle un encadrement strict afin d'en vérifier la qualité. Le droit de la non-discrimination ne peut, en effet, répondre à cette hypothèse de données biaisées, créatrices de discrimination. Enfin, il faut soulever une dernière difficulté, qui est l'insécurité et l'illisibilité de ce corpus juridique. La liste des critères punis en droit pénal s'allonge au gré des réformes législatives, ce qui ne manque pas de troubler l'appréhension globale de ce principe ; et l'action en justice menant à la sanction d'une discrimination relève de l'exploit, car la qualification matérielle de la discrimination et la preuve de son intention constituent un véritable défi. Dans le cas d'un algorithme prédictif, le défi ne peut en être que doublé.

Apporter la preuve d'une distinction opérée entre les individus par une prédiction amène plusieurs questions : comment identifier un critère illégal dans un algorithme ? En son absence, peut-on mobiliser la notion de discrimination indirecte, qui permet de ne regarder que le résultat de la décision prise, et non les motifs ? Le contentieux relatif à ces points est très fourni, ce qui ne manque pas de brouiller un essai de résolution de ces questions. De même, prouver l'intention de discriminer est en pratique extrêmement complexe ; le cas de l'algorithme prédictif pose alors une question plus fondamentale : peut-il y avoir une intention derrière le traitement algorithmique ? Si oui, qui porte cette intention ? Ici encore, le niveau d'autonomie de l'outil oriente les potentielles réponses : l'algorithme « classique » appelle la responsabilité du concepteur, tandis que l'algorithme auto-apprenant soulève encore des difficultés sur ce point (notamment sur l'idée d'une responsabilité autonome). Ainsi, l'élément moral de l'infraction met encore à mal l'application de ce principe.

Face à ces différentes difficultés, des idées ont été avancées afin de pouvoir étendre l'application du principe de non-discrimination aux algorithmes. Le Conseil National du Numérique plaide pour un principe général de non-discrimination qui s'imposerait aux plateformes[403] (toujours dans une optique du droit de la consommation seul) tandis que le rapport remis par Cédric Villani

[403] Rapport du Conseil National du Numérique, *Ambition numérique, Pour une politique française et européenne de la transition numérique*, juin 2015, p.57.

contourne le terme de discrimination en évoquant un « désavantage particulier »[404]. OVNI du droit, cette expression peut sans doute être rapprochée du « déséquilibre significatif », notion de droit de la consommation[405] et de droit commercial[406], introduite dans le Code civil[407] à l'occasion de la récente réforme[408]. En revanche, ce déséquilibre n'a pas la même définition selon la branche du droit concernée. De ce fait, quid du droit des algorithmes prédictifs, lorsqu'aucun contrat n'est signé entre les parties (responsable de traitement et personne concernée par la prédiction) ? A l'image du déséquilibre significatif, le juge aurait ici un rôle à jouer dans la détermination d'indices permettant de conclure à un désavantage créé par la prédiction[409]. De cette façon, la notion de discrimination peut évoluer et le désavantage particulier pourrait répondre aux difficultés intrinsèques de la qualification de la discrimination. Mais ici le mille-feuille juridique n'est pas une solution satisfaisante.

Enfin, une dernière raison pour mettre de côté ce principe, concerne les biais présents dans les données ; le profilage qui se fonde sur ces données ne pourra que créer un profil tronqué de l'individu ciblé. Partant, des décisions discriminantes peuvent être prises en se basant sur ce profil tronqué. La problématique des biais présents dans les données soulève de nombreuses questions, et appelle à dépasser le cadre de l'interdiction classique des discriminations du droit français.

L'analyse des principes existants, susceptibles de pouvoir encadrer les risques de la prédiction, s'avère insuffisante. Face à cette lacune, il convient désormais de se questionner sur l'adaptation d'un principe déjà existant. C'est à cette fin que la transposition de la neutralité à la prédiction apparaît opportune.

---

[404] Rapport de la mission VILLANI, *Donner un sens à l'intelligence artificielle, Pour une stratégie nationale et européenne*, mars 2018, p.142.
[405] C. consom., art. L.212-1.
[406] C. com., art. L.442-6, I, 2°.
[407] C.civ., art. 1171 (dans le cas d'un contrat d'adhésion).
[408] Ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats.
[409] En suivant cette idée, la protection du consommateur dans le Code de la consommation viendrait (une fois de plus) déteindre sur le Code civil.

II) La consécration du principe de neutralité : outil d'encadrement de la prédiction

La transposition du principe de neutralité à la sphère des algorithmes n'est pas hasardeuse. La neutralité s'acclimate à la sphère numérique tout en venant combler les lacunes de la prédiction. A cette fin, elle requiert une définition qui lui soit propre **(A)**. Cette étape réalisée, il convient d'appréhender la prédiction et ses risques au travers du prisme de la neutralité **(B)**.

A) La transposition du principe de neutralité à la prédiction

Bien qu'existant dans de nombreux domaines[410], la neutralité renvoie le plus souvent à « *l'attitude d'impartialité du juge qui, exempt de toute idée préconçue, examine avec la même attention, les éléments favorables ou défavorables à chacune des parties* »[411]. La question de l'opportunité d'appliquer aux algorithmes la neutralité n'est pas sans raison.

L'étude d'un tel principe tire premièrement sa légitimité du constat d'adaptation à l'environnement numérique. Ce phénomène de transposition a déjà été amorcé par la neutralité technologique[412], ou plus récemment en 2015 à l'aide d'un règlement européen qui définit l'Internet ouvert[413]. Ces principes démontrent l'importance de la mutation du principe de neutralité aux spécificités de la sphère numérique afin de pouvoir être applicable.

Au même titre que la neutralité du net, si principe de neutralité de l'algorithme il devait y avoir, il bénéficierait d'une définition propre adaptée aux spécificités algorithmiques. Dès lors, une première ébauche du principe de neutralité de l'algorithme prendrait en compte les caractéristiques de celui-ci

[410] Par exemple, en droit international public, la neutralité s'intéresse à l'État « étranger à une guerre entre deux ou plusieurs autres États, [qui] s'abstient d'y participer ou d'assister l'un des belligérants ». Voir G. CORNU, Vocabulaire juridique, *op.cit*.

[411] *Ibid.*

[412] A. BLANDIN-OBERNESSER, « Le principe de neutralité technologique », in *Le droit de l'Union européenne en principes*, Ed. Apogée, 2006, Mélanges J. RAUX, p.243.

[413] Le principe de neutralité du net consiste à garantir cet internet ouvert, « *les utilisateurs finaux ont le droit d'accéder aux informations et aux contenus et de les diffuser, d'utiliser et de fournir des applications et des services et d'utiliser les équipements terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, et quels que soient le lieu, l'origine ou la destination de l'information, du contenu, de l'application ou du service, par l'intermédiaire de leur service d'accès à l'internet* ». Voir article 3 du règlement européen 2015/2120 du 25 novembre 2015 sur l'Internet ouvert.

ainsi que les finalités auxquelles il aspire. Partant, le principe de neutralité de l'algorithme renvoie au droit pour les utilisateurs de l'algorithme à un résultat non discriminant lorsque que celui-ci exécute les tâches fixées selon des paramètres destinés à éviter au maximum la survenance de biais dans son processus d'exécution. En réalité, tout l'intérêt de l'utilisation de l'expression « neutralité de l'algorithme » réside dans sa malléabilité[414], d'autant plus lorsqu'il est confronté au domaine encore partiellement maitrisé de la prédiction algorithmique. Cette expression générique est utile en ce qu'elle permet de traduire au mieux la finalité du principe qui en découle : tendre à assurer au mieux une représentativité neutre de l'algorithme exempte de tout biais.

La seconde raison justifiant la légitimité d'un tel principe repose sur la prise de décision qu'il entraîne. Outre leur personnalité juridique[415], les personnes soumises au principe de neutralité[416] partagent une autre caractéristique commune. Tant le fonctionnaire que le juge, ils sont amenés dans le cadre de leur fonction à prendre – ou aider à prendre dans le cas du médiateur – des décisions qui auront des effets sur la situation juridique d'individus. Le principe de neutralité est alors pensé comme une garantie de la qualité de leurs décisions[417]. Pour autant, un fonctionnaire, un juge ou un médiateur ne peuvent être neutres[418] notamment en raison de leurs convictions personnelles. Malgré cette réalité, cette obligation de neutralité demeure[419].

[414] Le parallèle peut être fait avec l'expression « justice prédictive ». Si elle fait l'objet de critique, cette expression est également saluée en raison de sa plasticité et de sa commodité malgré son ambiguïté technique ou sémantique. Voir Y. MENECEUR, « Quel avenir pour la justice prédictive ? Enjeux et limites des algorithmes d'anticipation des décisions de justice », *JCP G*, n° 7, 2018, p. 190.

[415] Exception faite du principe de neutralité du net implicitement consacré sans dire son nom par l'article 3 du règlement européen 2015/2120 du 25 novembre 2015 sur l'Internet ouvert.

[416] Il s'agit premièrement des magistrats, voir J.-L. MOURALIS, « Preuve : règles de preuve », *Répertoire de droit civil*, 2017 : « Aucun texte ne proclame sous cette forme le principe de la neutralité du juge. Il est cependant constamment affirmé par la doctrine ». Mais également des médiateurs, voir M.-E. VOLCKRICK, « Intervenir en tiers aujourd'hui », *Négociations*, 2007/1, p. 76.

[417] H. COLOMBET, A. GOUTTEFANGEAS, « La qualité des décisions de justice. Quels critères ? », *Droit et société*, dir. P. MBONGO, 2013/1, n° 83, p. 155 : Les auteurs évoquent l'indépendance et l'impartialité du juge comme garanties de la qualité des décisions en incluant la dimension de neutralité à celle d'impartialité.

[418] Concernant le fonctionnaire, voir P.-Y. MOREAU, « Si le fonctionnaire est un homme pensée et réalité du sujet dans l'administration entre 1900 et 1950 », *Droits,* 2016/2 (n° 64), p. 131.

[419] À titre d'exemple, en cas de manquement pour un fonctionnaire cela constitue une faute professionnelle. J. BERTHOUD, "La neutralité religieuse du fonctionnaire", *JCP A,* 2005, p. 1142.

S'il y a un consensus sur la nécessité d'éviter les biais algorithmiques[420], la question de la neutralité de l'algorithme est source d'une pléthore de critiques. La principale est l'impossibilité intrinsèque qu'un algorithme soit neutre[421]. Le code informatique n'est pas uniquement un outil technique transposant des calculs neutres, il est réalisé selon la perception de son concepteur[422]. Cette réalité soulevée, notamment par le Conseil d'Etat[423], n'est pas rédhibitoire à la consécration de la neutralité, dont l'application doit être encadrée[424]. Ce constat posé il faut réagir en conséquence.

Pour autant, ce constat est similaire s'agissant des juges, par exemple, mais auxquels la neutralité est toutefois appliquée. L'impossibilité de parvenir à un principe de neutralité pour les algorithmes peut également résulter des intérêts de ses concepteurs[425], notamment commerciaux[426]. Confronté à de tels intérêts, le principe de neutralité pourrait s'appliquer plus strictement pour les algorithmes de prédiction en matière de justice[427], de sécurité et s'appliquer plus souplement à l'égard d'acteurs privés.

Sans pour autant tomber dans l'excès de la chimère d'un algorithme parfaitement neutre, la neutralité de l'algorithme semble constituer une piste de réflexion intéressante comme moyen de lutte contre ces biais. La double critique dont elle fait l'objet ne nous semble pas suffisante pour écarter cette piste. Au contraire, le nombre de commentateurs qui évoquent – souvent d'un point de vue critique – la neutralité de l'algorithme semble aller en faveur de l'intérêt de la question voire de l'existence même de cette neutralité.

---

[420] Voir par exemple le rapport VILLANI précité sur la question de l'éducation, p. 190 : « *De même il importe de veiller à ce que ces dispositifs ne reproduisent aucun biais discriminant et luttent contre toutes formes de déterminisme social* ».

[421] Par exemple, Y. HARREL, expert auprès de l'Union Internationale des Télécommunications (UIT) et professeur en cyber stratégie, affirme que l'algorithme n'est jamais fondamentalement neutre (propos recueillis à l'occasion d'une interview par Sputnik en date du 22 novembre 2017).

[422] P. CORNILLE, « Justice prédictive : est-ce un oxymore ? », *AJFI*, juillet 2018, repère 7.

[423] J.-M. SAUVÉ, « La justice prédictive », Intervention lors du colloque organisé à l'occasion du bicentenaire de l'Ordre des avocats au Conseil d'État et à la Cour de cassation le 12 février 2018.

[424] *Ibid*. Le Conseil d'Etat se positionne pour la complémentarité du principe de neutralité avec le principe de transparence afin de pouvoir questionner le résultat des algorithmes de prédiction.

[425] R. GOLA, « Publicité digitale et encadrement des algorithmes », *Revue Lamy Droit de l'immatériel*, n° 141, 2017, p. 52.

[426] Rapport CNIL, op. cit., p. 29.

[427] Voir par exemple B. LAMON, « La profession d'avocat et la justice prédictive : un bel outil pour le développement du droit », *D.*, 2017, p. 808.

B) La neutralité : principe en germe pour encadrer les prédictions algorithmiques

Le principe de neutralité permet d'apporter des réponses aux différents risques que les algorithmes de prédiction peuvent entraîner. Pour cela, il permet d'imposer des étapes de contrôle *a priori* des algorithmes plutôt que de se focaliser seulement sur un contrôle *a posteriori*.

Malgré leur évolution exponentielle, les outils de prédiction ne peuvent prétendre à une fiabilité intangible. Chaque élément de son processus peut venir influencer le résultat. C'est en cela que le principe de neutralité doit s'appliquer à l'ensemble du processus d'élaboration, qu'il s'agisse des données **(1)**, du traitement algorithmique **(2)** ainsi que du résultat produit **(3)**.

Il faut toutefois souligner que la prédiction est une matière en constante évolution dont les risques n'ont pu être décelés de façon exhaustive.

1) La neutralité pour encadrer les données traitées

Les données, dans l'ingénierie de la prédiction, sont le socle sur lequel le résultat sera produit. Plus le nombre de données est important, plus le résultat pourra tendre à une importante fiabilité en raison du panel représentatif qui sera ainsi constitué. L'ère du *big data* offre un terrain propice à la prédiction. Pour autant, si la fiabilité du résultat dépend de la quantité de données, elle l'est tout autant de la qualité de celles-ci. En effet, les données traitées reflètent les biais cognitifs des individus, les comportements de la société, qui se répercuteront sur le résultat. Un exemple probant est celui de l'algorithme prédictif COMPAS. Utilisé par le service pénitentiaire au sein de plusieurs Etats américains, il permettait de donner le risque de récidive des détenus[428]. Aucun des critères n'était de nature discriminatoire. Le taux de récidive entre les populations de couleur de peau blanche et celles de peau noire était quasi-similaire[429]. Malgré ce constat, le nombre de faux positifs, c'est-à-dire de personnes évaluées comme ayant de fortes chances de récidiver mais qui ne

[428] J. ANGWIN, J. LARSON, S. MATTU, L. KIRCHNER, « Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks », *ProPublica*, 23 May 2016.
[429] *Ibid*. : respectivement 67% et 63,8%.

l'ont pas fait, était deux fois supérieur pour les personnes de couleur noire. La source de ce biais a été identifiée comme résultant de l'existence de comportements discriminatoires par la police américaine en fonction de la couleur de peau des personnes, notamment dans les contrôles et arrestations effectués.

Face à ce risque, la neutralité pourrait imposer une obligation pour les utilisateurs d'algorithmes prédictifs de limiter au maximum les biais dans les données utilisées, ainsi que d'identifier les biais présents pour en limiter par la suite les répercussions néfastes dans les décisions qui seront prises en se fondant sur un tel résultat algorithmique[430]. Il est nécessaire encore d'utiliser les données avec une distance critique[431].

De plus, ce risque soulevé pourrait mener à créer une obligation afin de permettre aux individus, dont les données sont traitées, de les consulter, de les rectifier, de comprendre les critères du raisonnement qui leur est appliqué. Cette idée rejoint celle portée par le Conseil d'Etat[432], qui plaide pour une sorte de procédure juridictionnelle, c'est-à-dire que la personne pourrait disposer d'un droit de présenter ses observations sur le traitement mis en oeuvre, à l'instar des droits des parties lors d'une action en justice. Par conséquent, la présence de biais dans les algorithmes amène des obligations à la fois en amont et en aval du traitement.

Puisque les données d'apprentissage de l'outil peuvent aussi comporter des biais, certains postulent pour des obligations particulières envers le concepteur et l'entraîneur de l'algorithme : surveillance accrue des conditions de collecte des données, de qualité, tout au long du fonctionnement[433]. Ils doivent opérer un choix dans les données afin qu'elles respectent la diversité des cultures ou des groupes d'utilisateurs des systèmes.

[430] C'est notamment la position défendue par Cathy O'Neil : C. O'NEIL, TED Talk, « The era of blind faith in big data must end », avril 2017.
[431] Rapport Villani, op.cit., p.151.
[432] CE, op.cit., p.239.
[433] Rapport CERNA, *Ethique de la recherche en apprentissage machine*, juin 2017, not. [DON-1] Qualité des données d'apprentissage.

2) La neutralité pour encadrer le traitement algorithmique

La neutralité comme barrage à l'utilisation de critères discriminants.

Ici, la situation est celle dans laquelle un algorithme utilise des paramètres de raisonnement qui s'avèrent être discriminants, biaisés à l'égard des individus. Le cas concerne des paramètres réellement discriminants (par exemple, prendre en compte l'état de santé, les opinions de la personne), ou bien qui n'apparaissent pas discriminants, mais qui créent un résultat discriminant (par exemple, utiliser l'adresse du domicile des personnes). Dans ce dernier cas, il s'agit également d'apprécier l'adéquation entre la donnée utilisée et la finalité poursuivie par le responsable du traitement (principe de minimisation des données[434]).

En conséquence de ce risque potentiel, le principe de neutralité invite à considérer comment ces critères discriminants peuvent être éradiqués d'un algorithme prédictif. Dans ce but, une analyse d'impact du traitement qui soit menée afin d'apprécier les risques de discriminations pour les personnes concernées (personnes dont les données sont traitées) peut constituer une obligation adéquate. C'est ainsi que le Groupe de l'Article 29[435] définit les traitements pour lesquels l'analyse d'impact du RGPD est obligatoire[436] ; et c'est encore l'opinion défendue par le rapport Villani[437] (« *discrimination impact assessment* »).

Finalement, il peut être intéressant de prévoir une action particulière de la personne qui se trouve confrontée à une décision qui lui paraît discriminante, en lui procurant les moyens nécessaires pour s'y opposer. Cela peut passer par des opérations de *testing* de l'algorithme prédictif, qui sont recevables en droit pénal pour qualifier une décision discriminante[438], dans le cadre d'une action collective permettant à plusieurs victimes de mêmes pratiques de sanctionner la discrimination.

[434] Notamment RGPD, art. 5 §1 c).
[435] Lignes directrices, Groupe de travail Article 29 , concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est susceptible d'engendrer un risque élevé aux fins du règlement (UE) 2016/679, 4 oct. 2017.
[436] RGPD, art. 35
[437] Rapport Villani, op.cit., p.22.
[438] C. pén., art. 225-3-1.

La nécessité du principe de neutralité au sein des algorithmes de prédiction auto-apprenants.

L'évolution des algorithmes va de pair avec celle de leurs techniques d'apprentissage. Devenant automatiques, sous l'appellation de *machine learning*[439], ils constituent « *une rupture avec l'algorithmie classique. Cela marque le passage progressif d'une logique de programmation à une logique d'apprentissage* »[440]. Le risque que l'algorithme développe des biais par ces techniques est avéré. À titre d'exemple, il est possible de citer les algorithmes comprenant des boucles de réitération. Il s'agit d'une technique par laquelle les résultats fournis par l'algorithme sont réutilisés pour alimenter la base de données de celui-ci. Bien que la base de données initiale soit importante, un algorithme a vocation à être sollicité de nombreuses fois. Ainsi, tous les résultats qu'il fournit viendront alimenter cette base de données. Mais si certains d'entre eux sont biaisés et ce, indépendamment des données, la technique de la boucle de réitération viendra importer un biais au sein de la base de données. Ce phénomène de boucle a un effet d'accentuation exponentielle sur tout biais qui pourrait survenir.

Cette technique d'apprentissage à risque n'est pas isolée. Il s'agit notamment du *clustering,* qui fait partie des techniques d'apprentissage non supervisées au sein de la catégorie générale du *machine learning*. Son fonctionnement repose sur des données injectées à l'algorithme qui vont lui servir d'exemples, destinés à ce qu'il se construise lui-même ses propres modèles[441]. Cette technique est principalement utilisée avec des images. Il devra, par exemple, déterminer les caractéristiques visuelles d'un chat, d'un arbre ou d'une personne sur la base d'images variées. Les modèles sont réalisés par l'algorithme et sans intervention humaine. Bien que les concepteurs testent la fiabilité des modèles, il existe donc un risque non négligeable que les modèles dégagés par l'algorithme présentent des biais. Cette crainte ne doit toutefois pas conduire au rejet d'une telle technique. En effet, le *clustering*, bien que comportant d'importants risques de biais,

[439] Ce constat est visible même outre-Atlantique. Voir Reporte El impacto de la inteligencia artificial en el emprendimiento , *Endeavor*, juin 2018, p.43.
[440] Rapport VILLANI, *op. cit.*, p. 26.
[441] M. T. LAW, R. URTASUN, R. S. ZEMEL, Deep Spectral Clustering Learning , *University of Toronto Computer Science*, p. 1.

constitue une des méthodes d'apprentissage les plus répandues[442] et les plus performantes. À son appui, la prédiction devient envisageable pour des domaines comme la médecine, afin de prévenir « *les causes d'une maladie ou les risques de contamination ou de rechute* »[443]. Ces avancées en matière de santé doivent être accompagnées et protégées par le principe de neutralité. Plusieurs obligations, incombant tant aux médecins utilisant ces méthodes de prédiction qu'à leurs concepteurs, peuvent être imaginées. La première consisterait pour le médecin à faire remonter aux concepteurs les résultats et les raisons pour lesquelles un biais pourrait être présent. Un dialogue entre spécialistes permettrait une amélioration de la prédiction et une prévention, voire une correction des biais. Les concepteurs se verraient tenus de rectifier le modèle créé par l'algorithme. De plus, il faudrait ajouter à cela une obligation de réaliser des tests poussés au moment de la création de l'algorithme mais également imposer des contrôles réguliers de la fiabilité des modèles, notamment à l'ajout de nouvelles données.

La prédiction est un exercice qui devient de plus en plus autonome de la main humaine. Il est actuellement interdit qu'une décision soit prise sur le seul fondement d'un traitement automatisé de données[444]. Le principe de neutralité, par la prévention et la correction des biais, montre ainsi l'importance et l'utilité de maintenir une supervision humaine en matière de *machine learning*.

3) La neutralité pour encadrer le résultat de l'algorithme

La neutralité comme outil de questionnement de la prédiction.

[442] *Ibid*., *loc. cit*. À titre d'exemple, la plupart des algorithmes de *Deepmind* repose en partie sur la méthode du *clustering*.

[443] R. Di BELLECO, *D'un système de santé curatif à un modèle préventif grâce aux outils numériques*, Renaissance numérique, sept. 2014, p.72. Voir sur https://issuu.com/ronandibelleco/docs/lbsantepreventiverenaissancenumeriq.

[444] Article 10 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : aucune décision de justice ni autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité .

Malgré les obligations qui peuvent être imposées dans une optique de prévention des biais, la prédiction donnée n'est pas pour autant invulnérable aux biais. Le principe de neutralité doit continuer à s'appliquer même au moment de la livraison du résultat. Diverses obligations pourraient venir s'appliquer.

La première serait, comme pour ce qui est des traitements à risque développés précédemment, de le tester en le confrontant à de multiples situations pour lesquelles il a été programmé à répondre. L'examen qui serait effectué devrait être complet et couvrir le spectre des cas de figures auxquels il pourrait être confronté. Les concepteurs seraient alors en mesure de les étudier pour corriger les biais observables. Afin d'affiner l'étude des résultats, l'avis d'experts en la matière pourrait être requis. Il pourrait ainsi s'agir de juristes pour la justice prédictive, d'officiers des forces de l'ordre pour la prédiction d'infraction…

L'obtention d'une prédiction neutre a fait l'objet de théorie scientifique. Pour qu'un résultat soit neutre l'étape de la pondération au sein du traitement est fondamentale. Une fois la prédiction effectuée, un ajustement de la pondération peut être réalisé en s'organisant autour de trois mécanismes : la calibration des données, l'équilibrage des positifs et l'équilibrage des négatifs[445]. La calibration, tout d'abord, consiste à comparer les *outputs* de l'algorithme afin de comprendre « *quelles valeurs des paramètres d'entrée permettent d'obtenir certaines dynamiques ou certains motifs* »[446]. A l'image de l'obligation développée précédemment, les *outputs* sont étudiés. Toutefois, l'étude va plus loin en recherchant la compréhension du fonctionnement de l'algorithme et la corrélation entre les *inputs* et les *outputs*. Cette étape a pour objectif de corriger les critères pouvant entraîner un résultat biaisé ou discriminant. Les deuxième et troisième mécanismes dépendants l'un de l'autre sont l'équilibrage des positifs et celui des négatifs. Cela signifie que pour deux groupes différents, les résultats obtenus pour l'un des groupes doivent se refléter sur ceux du second groupe. Ce n'est seulement que dans les cas où ces

[445] M. KLEINBERG, « On algorithm and fairness », conférence du cycle Algorithmes du Collège de France, 16 janvier 2018.

[446] R. REUILLON, S. REY, C. SCHMITT, M. LECLAIRE, D. PUMAIN, « Algorithmes évolutionnaires sur grille de calcul pour la calibration de modelés géographiques », *Journées scientifiques mésocentres et France Grilles 2012*, Octobre 2012, Paris, France, p. 3.

trois conditions sont réunies que l'algorithme peut être considéré neutre, opérant un traitement équitable exempt de biais[447]. Si l'on compare ce schéma à celui de l'algorithme COMPAS[448], on se rend compte que la calibration a été effectuée mais la balance des positifs et des négatifs n'était pas équilibrée[449]. Les biais, précédemment évoqués, venaient donc de ce déséquilibre. Ce processus de contrôle de la pondération et des mécanismes l'ajustant doit incomber aux concepteurs.

Une fois ces diverses mesures prises en interne pour prévenir des biais, un contrôle extérieur pourrait être imposé. Cela pourrait être formalisé par une autorisation nécessaire à la mise en service de ces outils de prédiction. Il pourrait s'agir d'un contrôle judiciaire ou d'un contrôle par une autorité constituée d'experts à même de réaliser un contrôle effectif de l'algorithme prédictif et du respect du principe de neutralité.

Un risque d'atteintes aux droits et libertés.

Une prédiction produite par un algorithme peut amener à limiter voire supprimer l'exercice d'une liberté individuelle ou d'un droit. En se fondant sur une modélisation du comportement de l'individu, l'algorithme l'enferme dans ce modèle de comportement construit à un instant T à partir des données disponibles sur cette personne, généralement sans mise en perspective. La prédiction pourra ainsi décider de déplacements, actes, achats, par l'individu, avant qu'ils ne se produisent. Cet enfermement algorithmique n'est pas sans conséquence sur la liberté de penser, d'accès à l'information. Mais d'autres exemples illustrent que nombre de droits et libertés sont ainsi impactés : l'accès au logement, à l'emploi, à l'information, à la culture, à un procès équitable. Ce dernier exemple renvoie à une peine décidée par un algorithme prédictif à l'égard d'un prévenu, qui sera appréciée *a posteriori* par le juge pénal. Ici, pour rejeter la prédiction, le juge devra étoffer considérablement son

[447] M. KLEINBERG, *op. cit*.

[448] COMPAS est un algorithme prédictif dont la compétence est l'évaluation du risque de récidive de détenus. Il est utilisé par les services pénitenciers de certains Etats américains.

[449] Voir l'enquête *Propublica* précitée : Parmi les personnes ayant obtenu un fort taux de récidive, il y avait 45% de faux positifs chez les populations de couleur noire contre 23% chez les populations de couleur blanche. En revanche, parmi les personnes ayant obtenu un faible taux de récidive, les résultats sont inversés : il y avait 48% de faux négatifs chez les populations de couleur blanche contre 28% chez les populations de couleur noire.

argumentation, alors même que le résultat peut être biaisé. Autre exemple, la possibilité pour les annonceurs sur Facebook de limiter les annonces immobilières pour certaines catégories de personnes, excluant d'autres catégories de ces annonces de logement, s'avère illégale[450]. Encore, la pratique de différenciation tarifaire en fonction des acheteurs d'un produit Apple[451] apparaît encore comme une restriction de liberté, en déduisant de ce premier achat la situation économique de l'individu, qu'elle soit vraie ou fausse.

Le principe de neutralité peut apporter un début de réponse à ce risque créé par une prédiction, par exemple en imposant une analyse d'impact du traitement qui sera mis en œuvre, sur le plan des potentielles restrictions aux droits et libertés des personnes. Citons également l'article 22 du RGPD, qui donne le droit à la personne de demander des explications lorsqu'une décision automatisée entraîne pour elle des effets juridiques (et ainsi peut amener à limiter ses droits). La personne pourra aussi demander à s'y opposer. Dans la même veine, donner plus de contrôle aux individus est une piste sur laquelle il faut s'engager[452]. Déjà les droits prévus par le RGPD permettent un contrôle des individus sur leurs données personnelles[453], qui peuvent imposer plusieurs actions au responsable de traitement. L'hypothèse de prédictions algorithmiques justifie un élargissement de ce contrôle accordé à l'individu, puisque dans ce cas, ses libertés et droits sont grandement mis en danger par la prédiction. Face à un traitement discriminant, biaisé, qui atteint ses droits et libertés, l'individu pourrait agir, avec d'autres, au sein d'une action collective afin de faire condamner ce traitement illégal[454]. Du côté de l'utilisateur de l'algorithme prédictif, un audit par des tiers peut faire partie des obligations

[450] Facebook (still) letting housing advertisers exclude users by race, 21 nov. 2017, https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-nationalorigin.

[451] A. HANNAK, G. SOELLER, D. LAZER, A. MISLOVE and C. WILSON, « Measuring Price Discrimination and Steering on E-commerce Web Sites », Working Paper, Northeastern University, November 2014.

[452] Le droit de disposer de ses données personnelles existe déjà : « *Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi* » (article 1er, loi n°78-17 Informatique et libertés). L'enjeu est maintenant de rendre ce droit effectif.

[453] RGPD, *op.cit.* voir le droit d'accès (article 15), droit d'opposition (article 21), droit de limitation du traitement (article 18), droit à la portabilité (article 20), droit d'effacement (article 17), droit de rectification (article 16).

[454] Voir le rapport Villani, *op.cit.*

inhérentes à la neutralité, afin que l'outil puisse être évalué pour mesurer les effets des prédictions produites[455].

Le principe de neutralité apporte ainsi une protection aux individus sur lesquels la prédiction pourrait avoir des effets. Dans l'hypothèse où une prédiction biaisée entraînerait un dommage, dont la cause réside dans le non-respect des obligations du principe de neutralité tel qu'il est envisagé, la responsabilité des acteurs pourrait être engagée. Les individus doivent pouvoir obtenir des explications et une réparation pour le dommage causé. De l'autre côté, la neutralité permet également aux acteurs d'échapper à une action en responsabilité s'ils ont détecté des biais et pris les mesures adéquates envers les individus.

Bien que ce point apparaisse évident, il convient toutefois de rappeler que la finalité poursuivie par les concepteurs ou les propriétaires de l'algorithme ne doit pas être biaisée ou discriminante, ce qui dans le cas contraire engagerait encore leur responsabilité sur la base du non-respect du principe de neutralité.

L'importance de ce principe pour la qualité et la fiabilité d'une prédiction ainsi que pour l'encadrement des risques possibles est avérée. Il vient ainsi compléter l'ingénierie de protection des algorithmes au côté des principes de loyauté et de transparence.

[455] Voir les travaux de N. DIAKOPOULOS, in Technology Review, cité dans InternetActu, Comment rendre les algorithmes responsables ? H. Guillaud, http://www.internetactu.net/a-lire-ailleurs/comment-rendre-les-algorithmes-responsables/

Corrélation et Causalité

De l'automatisme de la causalité juridique à l'autonomie de la corrélation algorithmique

Melis ARAS

Docteur en droit public
Membre du CERDACC, Université de Haute-Alsace

Résumé :

La corrélation n'est pas la causalité. La corrélation n'est pas non plus un renoncement à la compréhension des causes. Il ne s'agit pas de deux notions antagonistes. L'incertitude causale du rapport corrélatif présent dans l'usage des algorithmes prédictifs représente néanmoins un sujet d'inquiétudes pour le juriste. Les enjeux de leur conciliation, en vue de considérer la corrélation algorithmique en tant que mode complémentaire de raisonnement, se discutent plus fréquemment à l'ère du *Big Data*. La contribution à cette discussion s'opère par le développement des deux aspects majeurs de cette problématique : les raisons qui justifieraient la conciliation de la causalité et la méthode de corrélation algorithmique, et les mesures nécessaires à l'adoption/l'appréhension de cette « nouvelle » méthode par le droit.

Abstract :

Correlation is not causality. Neither is correlation a renunciation of understanding of causes. These are not two antagonistic notions. Nevertheless, the causal uncertainty of the correlative rapport that is present in the use of predictive algorithms raises concerns for the lawyer. The issues of their conciliation, in order to consider the algorithmic correlation as a complementary way of reasoning, are discussed more frequently in the era of

Big Data. An effort to contribute to this discussion is made by searching for answers to questions centralized on two points: the reasons which justify the reconciliation of causality and the method of algorithmic correlation, and the measures necessary for the adoption / apprehension of this "new" method by law.

« […] *À dire vrai, Big Data signifie surtout le franchissement d'un seuil à partir duquel nous serions contraints (par la quantité, la complexité, la rapidité de prolifération des données) d'abandonner les ambitions de la rationalité moderne consistant à relier les phénomènes à leurs causes, au profit d'une rationalité que l'on pourrait dire post-moderne, indifférente à la causalité, purement statistique, inductive, se bornant à repérer des patterns, c'est-à-dire des motifs formés par les corrélations observées entre des données indépendamment de toute explication causale*. »

Conseil d'État, *Numérique et droits fondamentaux*, La Documentation française, 2014, p. 407-408.

L'algorithme concerne une procédure, un « *ensemble de règles opératoires dont l'application permet de résoudre un problème au moyen d'un nombre fini d'opérations »*[456]. Autrement dit, il s'agit d'une *« suite finie de règles et d'opérations permettant d'obtenir un résultat à partir d'éléments fournis en entrée* »[457]. Les algorithmes, désignant ainsi des créations intellectuelles, sont des produits de l'intelligence artificielle destinés à comprendre le fonctionnement de la cognition humaine afin de créer des processus cognitifs comparables à ceux de l'être humain[458]. Le but vise par conséquent à « *faire accomplir des tâches par une machine qui simule l'intelligence humaine* »[459].

[456] Larousse, « algorithme ».
[457] Conseil d'État, *Puissance publique et plateformes numériques : accompagner l'« uberisation »*, Rapport annuel de 2017.
[458] Rapport réalisé par C. Villani et autres, *Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne*, Mars 2018, p. 9.
[459] Conseil d'État, *Puissance publique et plateformes numériques : accompagner l'« uberisation »*, *op.cit.*

L'intelligence des algorithmes consiste à exploiter des quantités massives, complexes, relativement peu structurées, de données, autrement dit *Big Data*, dans un temps record, « *pour en faire surgir non pas des relations causales explicatives mais des corrélations statistiquement signifiantes entre des éléments a priori sans rapport* »[460].

Un algorithme fonctionne soit à partir d'une liste de règles appliquées de manière automatisée (algorithme d'automatisation), soit en conceptualisant lui-même ses propres règles par le biais d'une technique d'apprentissage (algorithme d'apprentissage)[461]. En effet, le raisonnement de manière automatisée n'a rien de nouveau. Notamment, en matière de prévention des risques, des modèles mathématiques qui reposent sur des algorithmes sont déjà conceptualisés et utilisés par l'homme. Cependant, si jusqu'à présent il était question d'appliquer ces méthodes à des systèmes techniques, de nos jours elles se développent pour modéliser le comportement humain dans le processus décisionnel. De plus, les algorithmes d'apprentissage (*machine learning*) possèdent la capacité de s'adapter à des situations et d'évoluer en continu[462]. Cela leur confère une certaine autonomie, sans automatisme, par rapport à la décision finale, car ils progressent par corrélations et par inductions. Ils « *se gouvernent par leurs propres lois* »[463].

Les algorithmes n'étant de fait pas nouveaux, il s'agit de l'évolution de la façon de croiser des quantités massives de données. Une évolution se constate également dans les matières touchées par ces avancées technologiques. Ainsi, la « justice prédictive », se traduisant par un ensemble d'instruments développés grâce à l'analyse de grandes masses de données de justice, propose aujourd'hui, à partir d'un calcul de probabilités, de prévoir l'issue d'un litige[464]. La méthode prédictive fonctionnant par corrélation algorithmique trouble précisément le juriste au moment de l'établissement de la relation causale, au-delà de laquelle découlent également les problématiques liées à l'imputation

[460] Conseil d'État, *Numérique et droits fondamentaux*, *op.cit.*, p. 408.
[461] R. HINDI, « Algorithmes, intelligence artificielle : quelles définitions ? », in *Table-ronde : Des algorithmes et des hommes*, CNIL, 23 janv. 2017. V. également : Rapport « France Intelligence artificielle », mars 2017, p. 22 et s.
[462] E. SCARAMOZZINA, « Les enjeux juridiques du *big data* », *Jusristourisme*, 2017, n° 201, p. 35.
[463] Larousse, « autonomie ».
[464] B. DONDERO, « Justice prédictive : la fin de l'aléa judiciaire ? » *D.* 2017, p. 532. V. aussi A. GARAPON, « Les enjeux de la justice prédictive », *JCP G*, N° 5, 30 Janvier 2017, doctr. 31 ; J. DUPRÉ, J. L. VÉHEL, « L'intelligence artificielle au service de la valorisation du patrimoine jurisprudentiel », *Dalloz IP/IT* 2017 p. 500.

des responsabilités en cas de dommage. La causalité, « *rapport qui unit la cause à effet* »[465], n'est pas la corrélation, « *relation existant entre deux notions, deux faits, dont l'un appelle logiquement l'autre* »[466], dans laquelle le lien causal existe avec ou sans la réciprocité. La différence entre ces deux notions s'explique aussi par la définition de la notion de « cause » en droit. Considérée comme l'élément générateur, la cause signifie par extension « *le fondement, le motif, la raison* » ; voire, « *l'intérêt de l'acte juridique (pour son auteur)* »[467]. Ainsi, le rapport énoncé dans la définition de la notion de causalité, est un rapport explicable, traçable, et surtout compréhensible et accessible, en principe, pour tout individu. Ce caractère s'avère indispensable au sens strict, à l'établissement du lien de causalité pour le régime juridique de la responsabilité, notamment en droit privé ; il se montre en outre indispensable, au sens large, à l'acceptabilité de la décision, au respect de la sécurité juridique et de l'égalité des justiciables. Quant au « lien causal » qui existe dans la définition de la notion de corrélation, il s'agit d'un lien établi à l'issue de la méthode algorithmique, difficilement accessible du fait du codage informatique, et acceptable pour le public à défaut de la compréhension de l'établissement de la causalité. En bref, l'existence des corrélations n'implique pas qu'il y ait causalité entre les variables corrélées, et ne restitue pas de fait, en l'état, le raisonnement juridique.

Cependant, il ne s'agit pas de deux notions antagonistes. Bien que l'on constate une différence de conception entre les notions de causalité et de corrélation, une part de « causalité » en termes de conséquences existe dans la notion de corrélation. En effet, il faut bien distinguer le résultat issu de l'utilisation des algorithmes (élément substantiel) de la manière dont on parvient à ce résultat (élément procédural). Cette distinction produit fictivement deux catégories de personnes en la matière : le concepteur et l'utilisateur. Le concepteur est celui qui se trouve à l'initiative de l'algorithme (programmation initiale) ; l'utilisateur se sert de l'objet technique dont l'action est dictée par l'algorithme (maniement de l'outil algorithmique). Le rapport corrélatif n'est présent qu'entre les données utilisées dans la conceptualisation des algorithmes. Cela étant, ces données sont liées, « corrélées », entre elles en

[465] Larousse, « causalité ».
[466] Larousse, « corrélation ».
[467] *Vocabulaire juridique*, sous la direction de G. Cornu, Association Henri Capitant, Quadrige, PUF, 2018, p. 154.

suivant une certaine logique, une « cause », dans la mesure où l'algorithme se voit conçu d'une certaine façon. En outre, la décision de l'utilisateur pour appliquer ou non le résultat à l'issue de ce processus constitue une sorte de « causalité » entre son choix et les éventuelles conséquences qui en découlent. À cet égard, le droit réfléchit déjà aux différentes hypothèses de l'imputation de la responsabilité en cas de recours à l'outil algorithmique[468]. Sans tenter de faire assimiler la notion de corrélation à celle de causalité, le droit devrait adopter cette nouvelle méthode de « raisonner » pour se mettre à jour, pour s'adapter à l'évolution de la société. Ainsi, la conciliation des notions s'avère nécessaire et cela de manière encore plus urgente au vu de la vitesse de la technologie numérique. Cette conciliation constituerait également une réponse aux éventuelles imperfections de l'automatisme de la causalité juridique (**I**). La préparation du terrain juridique à la réception de la donnée technique ne doit pourtant pas être effectuée sans prévoir au préalable les mesures nécessaires à l'appréhension de l'autonomie de la corrélation algorithmique (**II**).

I) La corrélation au secours de la causalité juridique

La causalité juridique n'est pas la causalité scientifique[469], mais une causalité qualifiée. Elle dérive de la causalité scientifique (cause réelle), mais elle résulte de la qualification juridique des événements par le recours aux différentes théories de la causalité par le juriste, à l'instar de la « *théorie de la proximité de la cause* », de la « *théorie de l'équivalence des conditions* », de la « *théorie de la causalité adéquate* »[470]. La causalité juridique est imparfaite comparée à la causalité scientifique en considération de la cause réelle d'une situation, ce qui confirme « *le caractère approximatif des règles juridiques* »[471]. La causalité scientifique fonctionne par automatisme, sans intervention de la volonté, de l'intention, de l'interprétation. Bien qu'une certaine qualification de la causalité soit présente dans la détermination de la causalité en droit (lien de causalité), cette dernière agit également avec une sorte d'automatisme pour ne pas

[468] V. L. GODEFROY, « Le code algorithmique au service du droit », *D.* 2018 p. 734 ; « Algorithmes - Les algorithmes : quel statut juridique pour quelles responsabilités ? », *Communication Commerce électronique*, n° 11, Novembre 2017, étude 18.

[469] C. RADÉ, « Causalité juridique et causalité scientifique : de la distinction à la dialectique », *D.* 2012, p. 116.

[470] V. M. DEGUERGUE, *JCA*, fasc. 830 préc.

[471] J. PATARIN, *Le problème de l'équivalence juridique des résultats*, Thèse imprimée, Université de Paris, Faculté de Droit, Maurice Lavergne Imprimeur, 1951, pp. 10-11.

dénaturer la cause réelle. C'est la raison pour laquelle les différentes théories de la causalité adoptent un langage plutôt scientifique. Cela dit, le raisonnement dans la formation de la causalité juridique suit différentes étapes (de la causalité matérielle à l'imputation), qui ne sont nécessairement pas liées entre elles. La relation causale peut être établie de façon « orientée » (dans l'optique de l'imputation du fait dommageable à une personne paraissant la mieux à même d'endosser la responsabilité)[472]. La causalité juridique est une causalité qui « *peut se le permettre* »[473] dans l'objectif de parvenir à la « cause » la plus raisonnable, la plus légitime, la plus authentique, et par conséquent de rendre la décision la plus juste, la justice. En ce sens, l'automatisme de la causalité juridique est un automatisme relatif. À la relativité de l'automatisme de la causalité juridique s'ajoutent encore les cas de la distorsion de la causalité qui entravent l'achèvement des procédures de responsabilité.

Aujourd'hui, avec l'incertitude des temps modernes, l'effectivité de l'automatisme de la causalité juridique apparaît de plus en plus discutable. Au-delà de la méthodologie, le droit oblige à évoluer pour surmonter les difficultés liées à « l'insuffisance substantielle »[474] de la connaissance de cause (causalité scientifique). Notamment dans le domaine des enjeux de la santé environnementale, une certaine adaptation existe déjà en droit dans la détermination de la relation causale.

En matière de santé, le contentieux vaccinal démontre parfaitement l'évolution du raisonnement juridique dans la formation du lien de causalité. Le Conseil d'État, dans un arrêt du 9 mars 2007, reconnaît l'existence d'un lien de causalité entre la vaccination anti-hépatite B et la survenance d'une sclérose en plaques en se fondant sur le constat d'une non-exclusion d'un tel lien par les experts et en présence des circonstances particulières de l'espèce[475]. En la matière, la Cour de cassation introduit un assouplissement des exigences posées pour l'établissement du lien de causalité entre la sclérose en plaques et la vaccination[476]. La Cour estime que « *le doute sur la causalité scientifique peut*

[472] F. LEDUC, « Causalité civile et imputation », *RLDC*, suppl. au n° 40, 2007, 2631.
[473] P. BRUN, « Causalité juridique et causalité scientifique », *RLDC*, suppl. au n° 40, 2007, 2630.
[474] On peut encore ajouter la notion d'existence (existence substantielle), en considérant que l'explication causale insuffisante est assimilée à l'inexistence de la cause.
[475] CE 9 mars 2007, *M^me^ Schwartz*, req. n° 267635.
[476] Cass. 1^re^ civ., 22 mai 2008 (5 arrêts).

être juridiquement dépassé par le recours en l'espèce à des présomptions de fait graves, précises et concordantes, pour établir une causalité juridique »[477]. Ainsi, en l'absence de certitude scientifique pour l'établissement d'une relation causale entre la vaccination anti-hépatite B et la sclérose en plaques, une simple présomption, pourvu qu'elle soit « grave, précise et concordante », suffit à surmonter l'imperfection causée par l'automatisme de la causalité. Dans un contre-exemple, la Cour de cassation rejette le pourvoi formé par une patiente au motif « *qu'ayant apprécié la valeur et la portée des éléments de preuve qui lui étaient soumis, la cour d'appel a estimé souverainement qu'en l'absence de consensus scientifique en faveur d'un lien de causalité entre la vaccination et les affections démyélinisantes, le fait que Mme X ne présentait aucun antécédent personnel ou familial et le fait que les premiers symptômes étaient apparus quinze jours après la dernière injection ne constituaient pas des présomptions graves, précises et concordantes en sorte que n'était pas établie une corrélation entre l'affection de Mme X et la vaccination* »[478]. En la matière, la Cour de Justice de l'Union européenne (CJUE), en dépit de l'article 4 de la directive du 25 juillet 1985 sur la responsabilité du fait des produits défectueux, ne s'oppose pas à ce que le juge ait recours à des présomptions, à condition qu'il ne retienne pas une véritable présomption de droit en considérant comme toujours établi le lien de causalité[479].

Dans l'usage des présomptions, le droit fait recours au principe de précaution lorsqu'aucune preuve scientifique ne démontre le lien de causalité. Concernant certaines maladies, la preuve du lien de causalité se montre difficile à établir en raison de l'absence d'un facteur unique responsable de la maladie en question. Il en va ainsi des maladies multifactorielles, tel est le cas lorsqu'il est impossible d'établir un lien de causalité scientifiquement certain entre l'exposition aux rayonnements ionisants résultant des essais nucléaires et le cancer dont souffre le demandeur. Cela étant, en matière nucléaire, un régime d'indemnisation existe depuis la loi du 5 janvier 2010 établissant une présomption de causalité pour tout demandeur justifiant, d'une part, avoir résidé ou séjourné dans l'une des zones et aux dates précisées par la loi et, d'autre part, avoir développé l'une des maladies dont la liste a été fixée par

[477] A. ROUYERE, « Variations jurisprudentielles à propos du lien de causalité entre vaccination contre l'hépatite B et sclérose en plaques », *RFDA* 2008 p. 1011.
[478] Cass. 1re civ., 25 nov. 2010, n° 09-16.556.
[479] CJUE, 21 juin 2017, aff. C-621/15.

décret[480]. Dans un arrêt du Conseil d'État du 12 avril 2013, le principe de précaution est ainsi appliqué pour reconnaître l'existence d'un risque accru de leucémie chez l'enfant lors d'une exposition résidentielle à des champs électromagnétiques de très basse fréquence[481], et cela en établissant une « corrélation » entre la résidence dans l'environnement proche d'une ligne à très haute tension et la survenance, supérieure à la moyenne, de leucémies chez l'enfant[482]. Le contentieux environnemental pose de la même manière la question du lien de causalité, qui a d'ailleurs conduit à l'utilisation de présomptions tant par le juge français que par le juge européen[483]. La difficulté dans la preuve du lien de causalité provient, comme dans les cas de maladies multifactorielles, de la présence des facteurs multiples, variés et souvent difficilement identifiables entraînant des désagréments environnementaux.

Outre les enjeux de santé environnementale, il paraît également probable que le caractère de certitude du lien de causalité ne soit pas toujours apprécié avec rigueur par la jurisprudence. À titre d'exemple, en matière de droit de la concurrence, le demandeur à l'action en concurrence déloyale doit, en principe, démontrer l'existence d'un lien de causalité entre la faute et le dommage pour lequel il demande réparation. Toutefois, les juges du fond comparent généralement l'évolution des chiffres d'affaires des deux entreprises pour constater une « *corrélation entre l'installation concurrente et la diminution du chiffre d'affaires* » de la victime des procédés déloyaux[484]. La jurisprudence qui établit la preuve du préjudice dans celle du comportement

[480] V. loi n° 2010-2 du 5 janvier 2010 relative à la reconnaissance et à l'indemnisation des victimes des essais nucléaires français, *JORF* n°0004 du 6 janvier 2010 p. 327. M. LAMOUREUX, « Le nouveau régime d'indemnisation des victimes des essais nucléaires », *Énergie - Environnement – Infrastructures*, n° 11, Novembre 2017, étude 25. V. également M. LAMOUREUX, « La causalité juridique à l'épreuve des algorithmes », *JCP* 2016. 731.

[481] CE, Ass., 12 avril 2013, *Association coordination interrégionale Stop THT et autres*, n° 342409, cons. 38. V. O. CACHARD, « La preuve des risques associés à l'exposition aux champs électromagnétiques », *JCP G*, n° 37, 11 Septembre 2017, doctr. 944.

[482] V. M. CANEDO-PARIS, « Des nouvelles du principe de précaution. À propos de l'arrêt du Conseil d'État, Assemblée, 12 avril 2013, *Association coordination interrégionale Stop THT et autres*, […] », *RFDA,* 2013 p. 1061.

[483] M. BACACHE, « Changement climatique, responsabilité civile et incertitude », *Énergie - Environnement – Infrastructures*, n° 8-9, Août 2018, dossier 30. V. également, F. GIANSETTO, « Le droit international privé à l'épreuve des nouveaux contentieux en matière de responsabilité climatique », *Journal du droit international (Clunet)*, n° 2, Avril 2018, doctr. 6.

[484] Y. PICOD, Y. AUGUET, N. DORANDEU, « Concurrence déloyale », *Répertoire de droit commercial*, oct. 2010 (actu. sept. 2018), § 134-135.

déloyal écarte ainsi l'exigence de la démonstration du lien de causalité, car il est présumé.

Ces exemples témoignent non seulement de l'imperfection de la causalité juridique (par rapport à la causalité scientifique) mais aussi de son évolution vers une présomption de causalité. La causalité juridique à l'épreuve des algorithmes amène à certains parallélismes avec ces exemples dans lesquels la présence de multiples facteurs non traçables complique l'établissement du lien de causalité. Le fonctionnement des algorithmes se fonde également sur la présence de multiples critères à l'instar d'un algorithme classique de *scoring* pour un crédit bancaire. Les corrélations ne vont pas de la cause vers la conséquence, mais remontent des conséquences vers une estimation des causes probables[485]. Il faut reconnaître que la recherche de la « cause certaine » du fondement de la décision finale, l'idéal constant recherché, se trouve souvent limitée. Toutefois, il serait excessif d'envisager une présomption légale pour le cas de l'utilisation des algorithmes.

Le recours aux algorithmes calculant une probabilité de causalité devient nécessaire lorsque le lien causal est incertain. C'est la raison pour laquelle le caractère complémentaire de la méthode algorithmique ne doit pas être sous-estimé par le juriste. Néanmoins, cela ne peut s'envisager qu'en prévoyant des mesures nécessaires au bon fonctionnement de la méthode.

II) La causalité juridique en support de la corrélation algorithmique

Les évolutions technologiques, *chose technique,* dès leur genèse, sont destinées à être soutenues par divers domaines juridiques, *chose juridique*. Les dispositions juridiques existantes sont mises à jour en fonction des nouveautés apportées par l'évolution de la chose technique. Or, la plupart du temps, l'incompatibilité entre la chose technique et la chose juridique (ré)apparaît en raison du « sens de l'interaction » existant entre ces deux « choses ». Il s'avère donc être nécessaire de l'inverser. La chose juridique doit être au service de la chose technique, d'abord pour l'appréhender, ensuite pour la structurer et consolider son exercice. La chose technique, à chaque fois qu'elle évolue, doit

[485] D. CARDON, *A quoi rêvent les algorithmes. Nos vies à l'heure des big data*, Le Seuil, 2015.

être intégrée dans la substance juridique. Les avancées technologiques doivent être accompagnées par une évolution juridique appropriée. Ainsi, pour considérer le recours à la corrélation algorithmique comme une nouveauté pour le raisonnement juridique, il faut que le droit l'adopte en son sein en prévoyant des mesures tant en amont (conceptualisation des algorithmes) qu'en aval (utilisation des algorithmes) du processus et cela sans négliger les conséquences de leur utilisation, notamment en termes de responsabilités.

La conceptualisation des algorithmes, en particulier celle de ceux qui sont prédictifs, repose sur deux piliers, l'un quantitatif, l'autre qualitatif. L'aspect quantitatif consiste à établir des corrélations sur une base comportant des données massives. Quant à l'aspect qualitatif, la modélisation de ce grand nombre de données implique la catégorisation et l'interprétation de ces données produisant des résultats déterminés[486]. Le Conseil d'État, dans son étude annuelle de 2014 sur le numérique et les droits fondamentaux, énumère certains objectifs pour encadrer, dès leur conceptualisation, l'utilisation d'algorithmes prédictifs à l'égard des individus[487]. Concernant l'aspect quantitatif, la qualité des données et leur hiérarchisation représentent deux éléments essentiels permettant de profiter de la valeur intrinsèque des données, ce qui permettra également l'établissement d'un rapport de corrélation solide. Quant à l'aspect qualitatif, la transparence des procédés et le caractère explicable des algorithmes constituent de la sorte des conditions nécessaires à la « non-discrimination » des justiciables confrontés au traitement algorithmique[488]. Des recommandations de transparence sont présentes pour réguler le recours aux algorithmes dans la justice. Le rapport Cadiet de 2017 préconise, outre l'obligation de transparence, la mise en œuvre

[486] L.-M. AUGAGNEUR, « D'où jugez-vous ? Un paradoxe entre justice prédictive et réforme de la motivation des décisions », *JCP G*, n° 13, 26 mars 2018, p. 582.

[487] Ces objectifs sont les suivants : assurer l'effectivité de l'intervention humaine dans la prise de décision ; veiller à la non-discrimination ; mettre en place des garanties de procédure et de transparence ; développer le contrôle des résultats produits par les algorithmes. Conseil d'État, *Numérique et droits fondamentaux*, *op.cit.*, p. 237 et s.

[488] À cet égard, un avis de la Commission d'accès aux documents administratifs (CADA) du 16 septembre 2016 prescrit au ministère de l'Éducation nationale de communiquer le code source de l'algorithme « Admission post-bac », sur la saisine d'une association de lycéens qui dénonçait l'opacité du système. Avis n° 20161989 du 23 juin 2016. V. également J. ROCHFELD, « L'encadrement des décisions prises par algorithme », *Dalloz IP/IT*, 2018, p.474.

des mécanismes de contrôle par la puissance publique et l'adoption d'un dispositif de certification de qualité par un organisme indépendant[489].

S'agissant du droit à l'information, au stade de l'utilisation des algorithmes, des mesures nécessaires sont prévues par la loi du 7 octobre 2016 pour une République numérique[490]. D'après cette dernière, une décision individuelle prise sur le fondement d'un traitement algorithmique doit comporter une mention explicite pour informer l'intéressé. C'est une obligation de transparence également mentionnée à l'article L. 311-3-1 du Code des relations entre le public et l'administration[491]. Le décret du 16 mars 2017 relatif aux droits des personnes faisant l'objet de décisions individuelles prises sur le fondement d'un traitement algorithmique précise les principales caractéristiques de l'algorithme à transmettre par l'administration à l'intéressé, si celui-ci en fait la demande. L'accessibilité aux algorithmes se révèle également nécessaire pour diminuer l'asymétrie d'information qui existe entre le concepteur et l'utilisateur. Cela dit, le caractère explicable, l'« explicabilité » des algorithmes reste encore un défi et cela même pour les concepteurs dès lors qu'il s'agit de l'apprentissage par la machine[492]. Au-delà d'un droit à l'information, un « droit à l'explication » s'avère nécessaire pour l'acceptation sociale du recours aux algorithmes comprenant à la fois la pertinence et la représentativité des données, la fiabilité de leur collecte, et l'objectivité de la modélisation de l'algorithme.

L'acceptation sociale du recours aux algorithmes se trouve en outre liée à l'imputation des responsabilités en cas de dommages. Différents régimes de responsabilité sont déjà examinés par analogie afin de les transposer au cas des algorithmes[493]. Toutefois, une telle transposition aboutirait à des solutions impertinentes en raison du caractère immatériel des produits issus de l'intelligence artificielle et de leur autonomie décisionnelle, comme il en va

[489] Mission d'étude et de préfiguration confiée au professeur Loïc CADIET, *op.cit.*, p. 25.
[490] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, *JORF* n°0235 du 8 octobre 2016.
[491] V. l'art. 39 de la loi informatique et liberté de 1978 qui dispose que toute personne a le droit d'obtenir les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. V. également l'art. 22 du règlement 2016/679 sur la protection des données personnelles.
[492] Conseil d'État, *Numérique et droits fondamentaux, op.cit.*, p. 235.
[493] H. PAULIAT, « La décision administrative et les algorithmes : une loyauté à consacrer », *RDP*, n° 3, p. 641. V. également : J.B. DUCLERCQ, « Les algorithmes en procès », *RFDA* 2018, p. 131 ; M. CLÉMENT, « Algorithmes au service du juge administratif : peut-on en rester maître ? », *AJDA* 2017, p. 2453 ; F. MELLERAY, « La justice administrative doit-elle craindre la justice prédictive ? », *AJDA* 2017, p. 193.

pour les régimes de responsabilité du fait des choses[494] ou du fait des animaux[495].

S'agissant des algorithmes d'apprentissage, l'autonomie décisionnelle représente une source d'indétermination en matière d'imputation de la responsabilité, car l'origine du comportement dommageable se montre difficile à identifier s'il ne relève pas de sa conception (une faute dans la programmation initiale) ou de son utilisation (une mauvaise utilisation)[496]. Cette difficulté se voit également constatée dans une résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique : « […] *dans l'hypothèse où un robot puisse prendre des décisions de manière autonome, les règles habituelles ne suffiraient pas à établir la responsabilité juridique pour dommages causés par un robot* […] »[497]. Par conséquent, une certaine part d'imprévisibilité existe dans les « comportements » des algorithmes d'apprentissage. Du fait de cette éventuelle imprévisibilité, on peut considérer la responsabilité objective comme le régime de responsabilité le plus pertinent en la matière. Le Parlement européen préconise, d'ailleurs, dans sa résolution la responsabilité objective pour le futur instrument législatif en matière de responsabilité civile pour les dommages causés par les robots, en mettant l'accent notamment sur « *la preuve des dommages causés et de la relation de cause à effet entre les dommages causés à la partie lésée et le fonctionnement dommageable du robot* »[498]. Ainsi, la causalité, bien qu'absente tout au long du processus décisionnel inhérent aux algorithmes d'apprentissage (car ils fonctionnent par corrélation et sont autoapprenants), se trouve naturellement présente dans les usages de ces derniers. Ladite résolution, dans son passage relatif aux principes éthiques, insiste à cet égard sur le principe de transparence : « *à savoir qu'il devrait toujours être possible de fournir la justification rationnelle de toute décision prise avec l'aide de l'intelligence artificielle qui est susceptible d'avoir une incidence importante sur la vie d'une*

[494] J.-M. BRUGUIÈRE, « Droit à l'oubli des internautes ou... responsabilité civile des moteurs de recherche du fait du référencement ? Retour sur l'arrêt de la CJUE du 13 mai 2014 », *Resp. civ. et assur*., 2015, étude 5.
[495] N. NEVEJANS, *Traité de droit et d'éthique de la robotique civile*, LEH éditions, 2017.
[496] J.-P. DESBIOLLES, « Algorithmes, intelligence artificielle : quelles définitions ? », in *Table-ronde : Des algorithmes et des hommes,* CNIL, 23 janv. 2017.
[497] Résolution du Parlement européen du 16 févr. 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique.
[498] Résolution du Parlement européen du 16 févr. 2017 […], pt. 54.

ou de plusieurs personnes […] »[499]. L'instauration d'un nouveau régime juridique propre aux algorithmes n'est pas envisageable sans prévoir une obligation de transparence dès sa conceptualisation sur laquelle se fonderait le régime de responsabilité[500].

Enfin, la chose technique constitue le moteur, la motivation, d'une évolution juridique en devenir. Pourtant, ce n'est pas la chose technique qui consacre cette évolution juridique. Le droit doit être au service de la technique. Dans le cas contraire, la chose technique ne peut qu'ajouter de nouvelles problématiques au régime juridique de son domaine d'application. Ainsi, pour pouvoir privilégier un modèle déductif de corrélation sur un modèle de causalité, certains facteurs, tels que « le principe d'appréciation souveraine du lien de causalité », « l'admission de la preuve par présomption » et « la préférence rationnelle pour la vérité calculée plutôt que l'ignorance », devraient se combiner[501]. La fonction performative des algorithmes prédictifs pourrait par conséquent servir au droit dans la création des réalités[502], par sérendipité, contribuant à la connaissance des causes « inconnues ». Le droit doit, par conséquent, préparer le terrain adéquat pour la maturation de l'évolution de la chose technique. L'objectif consiste, notamment, à conserver une approche préventive dans la réponse du droit face aux éventuelles ruptures. Cette approche doit également avoir pour but de tirer les bénéfices des évolutions technologiques. Par conséquent, adapter le droit au fait signifie un choix politique à l'ère du numérique.

[499] Résolution du Parlement européen du 16 févr. 2017 […], pt. 12. V. également, CNIL, *Comment permettre à l'homme de garder la main. Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, décembre 2017.
[500] D. LE METAYER, « Transparence des algorithmes : quelles réponses juridiques et techniques », in *Algorithms : too intelligent to be intelligible ? 10th international conference on computers privacy and data protection*, Bruxelles, 25 janvier 2017.
[501] L.-M. AUGAGNEUR, « L'évaluation du préjudice concurrentiel à l'ère du Big Data », *JCP E*, n° 25, 18 juin 2015, p. 27.
[502] H. CROZE, « La factualisation du droit », *JCP G*, N° 5, 30 Janvier 2017, p. 175.