

Revue générale du droit, 2024

Aperçu sur les quelques actualités italiennes en droit de l'informatique et de l'administration électronique (juin 2022 – juin 2023)

Giorgio Mancosu¹

Citer cette publication : Giorgio Mancosu, « Aperçu sur les quelques actualités italiennes en droit de l'informatique et de l'administration électronique (juin 2022 – juin 2023) » Revue générale du droit, 2024.

¹ Professeur contractuel en droit public à l'université de Cagliari et chercheur associé au Centre de Droit Public Comparé de l'université de Paris 2.

Dans les douze derniers mois, ce sont quatre les actualités à même de donner le sens des pistes évolutives du droit de l'informatique (I) et de l'administration électronique (II) en Italie.

On peut globalement en tirer la leçon suivante : on pourra bien sûr s'attendre à des avancements après l'adoption du règlement UE sur l'intelligence artificielle², mais, à présent, le 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, et abrogeant la directive 95/46/CE (RGDP), et la jurisprudence qui l'enrichit, continue de faire office de Magna Charta en la matière. En d'autres termes, les outils juridiques ne font pas défaut et aujourd'hui c'est plutôt question de les approprier et d'en tirer tout le potentiel pour accomplir les missions traditionnelles du droit de l'informatique : régler les conflits d'intérêts relatifs à l'utilisation des technologies informatiques ; empêcher l'utilisation des technologies informatiques à l'encontre des valeurs juridiques ; promouvoir l'utilisation des technologies informatiques pour (mieux) satisfaire les droits individuels et collectifs³.

Néanmoins, on ne devrait pas se faire trop d'illusions. Comme nous le montrent notamment les deux actualités en droit de l'informatique, force est de constater que la compétence territoriale du droit de l'UE est

2 Proposition de règlement du Parlement Européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union.

Fiche de procédure : [https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=fr&reference=2021/0106\(COD\)](https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=fr&reference=2021/0106(COD)).

Voir les amendements du Parlement européen, adoptés le 14 juin 2023, à la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) : https://www.europarl.europa.eu/doceo/document/A-9-2023-0188_FR.html. L'adoption de cette position de négociation par le Parlement européen a ouvert maintenant les discussions avec les États membres sur la forme finale de la législation. B. Jeulin, « Amendement de l'Artificial Intelligence Act : la théorie confrontée à la pratique », Dalloz actualité, juin 2023.

3 G. Sartor, *L'informatica giuridica e le tecnologie dell'informazione: corso d'informatica giuridica*, Torino, Giappichelli, 2016.

toujours mise à mal par l'étendue mondiale des réseaux, des services et du public visé.

I. Droit de l'informatique

En droit de l'informatique, les actualités illustrées ci-après portent toutes les deux sur la mise en tension du RGPD, notamment du côté de son effectivité et de son champ d'application territoriale.

A. ChatGPT *versus* le RGPD : premier round

À la suite d'une violation de données, qui lui a été signalée le 20 mars dernier, l'autorité de contrôle italienne a prononcé le 30 mars dernier une mise en demeure à l'encontre d'OpenAI, la firme basée aux Etats-Unis qui fournit l'application d'intelligence artificielle générative appelée ChatGPT (le fameux *chatbot* exploitant le modèle de langage appelé GPT - *Generative Pre-trained Transformer* - pour créer du texte à partir d'instructions saisies par un utilisateur humain). C'est la première décision au monde à ce sujet qui, en l'espace de quelques jours, a convaincu même le Comité européen de la protection des données (CEPD) de mettre en place un groupe de travail spécialisé afin de développer une doctrine partagée au niveau européen⁴. En effet, l'autorité italienne a ouvert le bal des décisions, mais elle est loin d'être la seule : « *l'autorité allemande du land de Hesse a publié un article dans lequel elle indique partager les inquiétudes de l'autorité italienne ; l'autorité espagnole a annoncé avoir ouvert une enquête ; l'autorité catalane a publié des recommandations pour dissuader l'usage de ChatGPT dans l'exercice de fonctions publiques et la fourniture de services publics ; la CNIL ne s'est pas exprimée sur ChatGPT à ce stade, même si elle a été déjà saisie de plusieurs plaintes dirigées à l'encontre d'OpenAI* »⁵. Par ailleurs, la CNIL a publié un plan d'action pour le déploiement de systèmes d'IA, notamment des IA dites génératives⁶, et

4 Voir : https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en.

5 L. Dubois, « ChatGPT versus le RGPD – Point d'étape au 1^{er} mai 2023 sur l'actualité européenne », Dalloz actualité, mai 2023.

6 Voir : <https://www.cnil.fr/fr/intelligence-artificielle-le-plan-daction-de-la-cnil>.

le Laboratoire d'innovation numérique de la CNIL vient de publier un dossier qui leur est consacré⁷.

Pour comprendre les enjeux soulevés par la décision de l'autorité de contrôle italienne, quelques précisions sur le fonctionnement de ChatGPT s'imposent.

Le *chatbot* ChatGPT est une interface qui traite les informations renseignées par l'utilisateur via un algorithme de traitement du langage (appelé « Transformeur ») et présente la sortie de ce traitement sous un format compréhensible par l'utilisateur. La réponse fournie ne prétend pas à être vraie, mais elle ne constitue que le passage linguistique le plus statistiquement probable en réaction aux éléments linguistiques fournis en entrée. La fiabilité du résultat dépend des paramètres suivis par l'algorithme (on estime que la dernière version, GPT 4, compte environ mille milliards de paramètres), la précision de ces paramètres reposant sur l'application de techniques d'apprentissage supervisé et non supervisé appliquées à des quantités colossales de données.

ChatGPT tombe sous le RGPD dans la mesure où la conception de l'algorithme sous-jacent, d'une part, et l'interaction avec les utilisateurs, d'autre part, comportent des traitements de données à caractère personnel. En effet, la conception et l'affinement progressif du modèle de langage nécessite structurellement le traitement de masses colossales de données, peu importe leur caractère personnel ou anonyme. La plupart des données d'entraînement sont collectées sur le web : ce qu'on appelle moissonnage, ou *scraping*, de données. Quant à l'utilisation du système ChatGPT, elle comporte le traitement des données entrées par les utilisateurs lors de la conversation à deux fins : pour produire les réponses et pour améliorer les performances du modèle de langage, dans son ensemble.

Or, avant d'illustrer la décision de l'autorité de contrôle italienne, il faut rappeler que le but du RGPD n'est pas d'empêcher les traitements de données personnelles, mais d'assurer leur libre circulation, tout en donnant aux personnes physiques les moyens pour garder toujours le contrôle sur les données les concernant, car ces données sont considérées

⁷ Voir : <https://linc.cnil.fr/dossier-ia-generative-Chat-GPT-un-beau-parleur-bien-entraine>.

en même temps le carburant de l'économie numérique et les particules de l'identité personnelle (« ce que l'on sait de nous »). Comment le RGPD tente d'assurer l'arbitrage entre libre circulation des données personnelles et protection de l'identité des personnes physiques concernées ? Au biais d'un certain nombre de principes fondamentaux, tels que celui de licéité, finalité, transparence, minimisation, responsabilité, etc (art. 5).

L'autorité de contrôle italienne a notamment relevé les manquements suivants : 1) qu'aucune information n'ait été fournie aux utilisateurs, ni aux personnes concernées dont les données ont été collectées par OpenAI et traitées via le service ChatGPT (manquement au principe de transparence) ; 2) l'absence de base juridique appropriée en ce qui concerne la collecte de données à caractère personnel et leur traitement dans le but d'entraîner les algorithmes qui sous-tendent le fonctionnement de ChatGPT (manquement au principe de licéité) ; 3) que le traitement des données personnelles des personnes concernées est inexact car les informations fournies par ChatGPT ne correspondent pas toujours aux données réelles (manquement au principe d'exactitude) ; 4) l'absence de vérification de l'âge des utilisateurs par rapport au service ChatGPT qui, selon les termes publiés par OpenAI, est réservé aux personnes âgées de 13 ans ou plus (manquement aux conditions d'utilisation du service).

Globalement, l'autorité italienne présume la violation des articles 5, 6, 8, 13 e 25 du RGPD et, par conséquent, conformément à l'article 58, paragraphe 2, point f), du RGPD, en raison de l'urgence et dans l'attente de l'achèvement de l'enquête nécessaire, enjoint à OpenAI, avec effet immédiat, la limitation temporaire du traitement des données personnelles des personnes concernées établies sur le territoire italien. Le responsable du traitement est invité à communiquer, dans un délai de vingt jours, les mesures adoptées pour se conformer à la délibération de l'autorité. Il faut rappeler que, au sens de l'article 4 du RGPD, on entend par « limitation du traitement » : le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur. La limitation du traitement constitue en même temps l'une des mesures correctrices dont disposent les autorités de contrôle et un droit reconnu, dans certains cas, aux personnes concernées (art. 18). Selon le considérant 67, « Dans les fichiers

automatisés, la limitation du traitement devrait en principe être assurée par des moyens techniques de façon à ce que les données à caractère personnel ne fassent pas l'objet d'opérations de traitements ultérieures et ne puissent pas être modifiées ». Pour faire suite aux remarques de l'autorité de contrôle, OpenAI a choisi la voie techniquement la plus rapide du blocage de ChatGPT aux adresses IP italiennes, ce qui n'a rien à voir avec la limitation du traitement demandée par l'autorité de contrôle, qui consistait à « geler » les données sans considération des adresses IP des utilisateurs⁸.

Après d'intensives négociations avec les représentants de OpenAI, le 11 avril dernier l'autorité de contrôle italienne a considéré qu'il aurait été possible de suspendre la limitation temporaire du traitement à compter de la satisfaction d'un certain nombre d'exigences : 1) la publication d'un avis expliquant aux personnes concernées, y compris les personnes concernées autres que les utilisateurs du service ChatGPT, dont les données ont été collectées et traitées aux fins de l'entraînement des algorithmes : les méthodes de traitement, la logique qui sous-tend le traitement nécessaire au fonctionnement du service, leurs droits en tant que personnes concernées et toute autre information requise par le RGPD, dans les conditions et selon les modalités énoncées à l'article 12 du RGPD ; 2) la mise à disposition des personnes concernées, y compris celles qui ne sont pas des utilisateurs du service et qui se connectent depuis l'Italie, d'un outil leur permettant d'exercer leur droit d'opposition au traitement de leurs données personnelles, obtenues auprès de tiers, effectué par la société aux fins de l'entraînement des algorithmes et de la fourniture du service ; 3) la mise à disposition des personnes concernées, y compris celles qui ne sont pas des utilisateurs du service et qui se connectent depuis l'Italie, d'un outil leur permettant de demander et d'obtenir la rectification des données personnelles les concernant qui ont été traitées de manière inexacte dans le cadre de la génération des contenus ou, si cela est impossible en raison de l'état de la technique, l'effacement de leurs données personnelles ; 4) l'insertion dans le flux d'enregistrement d'un lien vers la notice d'information adressée aux utilisateurs du service, dans une position qui

⁸ Même s'il faut admettre que la question de la faisabilité technique de la mesure envisagée par l'autorité de contrôle est loin d'être tranchée.

permettre de la lire avant de procéder à l'enregistrement, de manière à permettre à tous les utilisateurs qui se connectent depuis l'Italie, y compris ceux qui sont déjà enregistrés, lors du premier accès suivant l'éventuelle réactivation du service, de lire cette notice d'information ; 5) la modification de la base juridique du traitement des données personnelles des utilisateurs aux fins de l'entraînement des algorithmes, en éliminant toute référence au contrat et en prenant comme base juridique du traitement le consentement ou l'intérêt légitime, en fonction des évaluations de l'entreprise dans une logique de responsabilisation ; 6) la mise à disposition sur le site web, au moins pour les utilisateurs du service qui se connectent depuis l'Italie, d'un outil facilement accessible grâce auquel ils puissent exercer leur droit d'opposition au traitement de leurs données acquises lors de l'utilisation du service pour l'entraînement des algorithmes si la base juridique choisie est l'intérêt légitime ; 7) à l'occasion de toute réactivation du service pour les utilisateurs basés en Italie, l'insertion d'une demande pour que ces derniers, y compris ceux qui sont déjà enregistrés, passent une barrière d'âge qui exclut, sur la base de l'âge qu'ils ont déclaré, les utilisateurs mineurs.

Avec un communiqué du 28 avril dernier⁹, l'autorité de contrôle italienne informe qu'OpenAI a mis en œuvre les mesures souhaitées par l'autorité, même si on attend toujours de savoir si et quand seront mises en œuvre les deux autres mesures demandées par l'autorité de contrôle : 1) la soumission à l'autorité, au plus tard le 31 mai 2023, d'un plan d'adoption d'outils de vérification de l'âge propres à exclure l'accès au service des utilisateurs de moins de 13 ans et des mineurs en l'absence de manifestation expresse de volonté de la part de ceux qui exercent la responsabilité parentale à leur égard¹⁰ ; 2) la promotion, au plus tard le 15 mai 2023, d'une campagne d'information, de nature non promotionnelle, sur tous les principaux médias italiens (radio, télévision, journaux et Internet), dont le contenu devra être convenu avec l'autorité, dans le but d'informer les personnes que leurs données personnelles sont susceptibles d'être collectées à des fins d'entraînement des algorithmes, qu'un avis

9 Voir : <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9881490>.

10 La mise en œuvre de ce plan devra débuter au plus tard le 30 septembre 2023.

d'information détaillé a été publié sur le site Web de la Société et qu'un outil a été mis à disposition, également sur le site Web de la Société, grâce auquel les personnes concernées peuvent demander et obtenir l'effacement de leurs données personnelles.

Cela dit, même s'il convient de saluer l'attention portée au sujet par l'autorité de contrôle italienne, on ne peut pas ignorer un problème largement non résolu et, peut-être, insoluble à ce stade : l'ineffectivité et le coût informatique et financier de mesures prises à posteriori, alors que la seule approche, techniquement efficace et juridiquement conforme, est celle de la « protection des données dès la conception et par défaut » (art. 25). Face à des services innovants tels que ChatGPT, qui, en l'espace de quelques mois, s'imposent à l'échelle mondiale, au point d'être déjà considérés comme incontournables par un très grand nombre d'utilisateurs, les mesures misant sur la transparence (à posteriori) et sur l'activisme des personnes concernées sont, il faut l'admettre, ridicules. Pour s'en rendre compte, il suffit de considérer que pendant les deux semaines où ChatGPT a été bloqué pour les adresses IP italiennes, les abonnements VPN pour contourner ce blocage se sont multipliés.

Pour s'en tenir à la protection des données personnelles, il faut admettre que ChatGPT et les autres solutions d'intelligence artificielle générative s'accommodent mal aux principes du RGPD, notamment dans la phase du paramétrage de l'algorithme. En attendant la doctrine du CEPD en la matière, on peut, par exemple, se demander comment, pendant l'entraînement de l'algorithme, faire droit au principe de finalité et à ses corollaires, tels que celui d'exactitude. Quant à la réutilisation des données personnelles diffusées spontanément sur la toile par les personnes concernées, comment évaluer si la nouvelle finalité poursuivie par ChatGPT est compatible avec la finalité de la diffusion ? Etant donné les différences entre le fonctionnement d'un moteur de recherche et celui des applications d'IA générative, comment « faire oublier » à ces dernières des imprécisions, des données obsolètes ou des données erronées concernant une personne identifiée ou identifiable ?¹¹ Il s'agit d'un enjeu de taille, car

11 « Un soir, le professeur de droit Jonathan Turley a reçu un e-mail troublant. Dans le cadre d'une étude de recherche, un collègue avocat en Californie avait demandé au chatbot Chat

il faut bien remarquer que ChatGPT (et tous les *chatbots* de ce type) n'est pas une base de données telle que la *cache* d'un moteur de recherche, ce qui fait que les informations qu'il produit ne peuvent pas être effacées, mais seulement rendues inaccessibles, à moins de bloquer l'ensemble du service. En effet, un système d'IA générative tire des enseignements des données, mais ne détient pas les données. À ce sujet, Luciano FLORIDI illustre, dans un article passionnant, les enjeux et les perspectives d'un domaine de recherche très récent en IA : « le désapprentissage automatique » (Machine Unlearning)¹² : « *Supposons que l'on demande à ChatGPT des informations*

GPT de générer une liste de juristes qui avaient harcelé sexuellement quelqu'un. Le nom de Turley était sur la liste. Le chatbot, créé par OpenAI, a déclaré que Turley avait fait des commentaires sexuellement suggestifs et tenté de toucher un étudiant lors d'un voyage scolaire en Alaska, citant un article de mars 2018 dans le Washington Post comme source d'information. Le problème : aucun article de ce type n'existait. Il n'y avait jamais eu de voyage de classe en Alaska. Et Turley a dit qu'il n'avait jamais été accusé d'avoir harcelé un étudiant », Wall Street Journal, 5 avril 2023 – Chat GPT a inventé un scandale de harcèlement sexuel et a nommé un vrai prof de droit comme accusé.

12 « La question qui se pose à ce stade est la suivante : en matière d'apprentissage automatique, une fois qu'un modèle a été formé, s'il y a un problème concernant la vie privée ou la propriété intellectuelle (ou la sûreté, la sécurité, le secret, etc.), existe-t-il une autre solution que (a) la suppression complète du modèle ; (b) la suppression des données indésirables de l'ensemble d'apprentissage et le réentraînement complet du modèle à partir de zéro ... ; ou (c) le "blocage" des informations qui ne devraient pas être obtenues, une fois que le modèle a appris à les produire ? La question est pressante car (a) peut facilement être trop radical ; (b) peut être très coûteux, financièrement, informatiquement et en termes de temps requis ; et (c) peut être totalement inefficace, de sorte qu'il dépend de l'importance de rendre l'information indisponible plutôt que simplement inaccessible. Heureusement, la réponse est un oui provisoire, car il existe une quatrième solution ... : le désapprentissage automatique (MU ...). D'un point de vue conceptuel, la MU n'est pas difficile à comprendre. En ML, les modèles sont formés sur des ensembles de données contenant des exemples du problème que le modèle est censé résoudre. Au cours de la formation, le modèle apprend à reconnaître des schémas dans les données disponibles et à faire des prédictions sur la base de ces schémas ou associations, en produisant les informations correspondantes. En fonction de l'ensemble de données - qui, par exemple, peut comprendre des données sensibles - le modèle peut apprendre des schémas ou des associations qui fournissent des informations inacceptables ou indésirables, pour des raisons épistémologiques (par exemple, parce qu'elles sont dépassées, inexactes, incorrectes ou trompeuses), éthiques (par exemple, parce qu'elles sont biaisées, injustes ou discriminatoires) ou juridiques (par exemple, parce qu'elles portent atteinte à la vie privée ou aux droits de propriété intellectuelle). La MU traite ces questions en supprimant du modèle toutes les traces de certains points de données (une sorte d'amnésie sélective), sans affecter les performances, de sorte que le modèle ne délivre plus les informations correspondantes qui posent problème. Ainsi, la MU peut être considérée comme l'inversion du processus qui a conduit un modèle à apprendre à fournir certaines informations spécifiques. Elle entraîne à nouveau le modèle de ML à fournir des informations avec une partie des données oubliées, afin de minimiser les coûts associés à un réapprentissage complet à partir de

financières sur la faillite de Mario Costeja González. En supposant que ChatGPT puisse répondre, il peut néanmoins bloquer la réponse, c'est-à-dire la rendre inaccessible, en expliquant que l'information n'est pas accessible en raison de la décision prise par la CJUE. C'est ce qui pourrait arriver (ou du moins devrait arriver) maintenant dans l'UE. En utilisant un langage très anthropomorphique, le ChatGPT "connaît" la réponse mais "refuse" de la fournir. Il s'agirait d'un compromis ... qui pourrait être rendu inutile par des solutions technologiques, telles que des messages-guides conçus pour tromper ChatGPT et l'amener à fournir l'information. Il serait préférable que ChatGPT ne connaisse pas du tout la réponse. Le Machine Unlearning pourrait y parvenir. Ainsi, dans un avenir proche, la CJUE pourrait exiger d'une entreprise qu'elle veille à ce qu'un chatbot désapprenne certaines informations spécifiques, ce qui les rendrait indisponibles en principe, et pas seulement inaccessibles en pratique. À l'avenir, les utilisateurs pourraient demander aux moteurs de recherche de respecter leur "droit à l'oubli" et aux systèmes de Machine Learning leur « droit à la désincarnation ».

Un autre enjeu extrêmement délicat est l'identification du fondement de licéité du traitement, notamment pour les données personnelles traitées à des fins de conception du modèle de langage. Le recueil du consentement étant matériellement impossible, OpenAI prône pour l'alternative suivante : « les intérêts légitimes poursuivis par le responsable du traitement »¹³. Or, le recours à ce fondement de licéité nécessite d'être dûment justifié, ce qui, à présent, est loin d'être le cas, comme l'autorité italienne vient elle-aussi de l'admettre dans un article de presse du 29 avril dernier¹⁴.

Enfin, une autre question capitale pèse sur le débat portant sur les services d'IA générative, lorsque les fournisseurs ne disposent d'aucun établissement dans l'Union européenne : l'applicabilité du RGPD au

zéro », Luciano Floridi, « Machine Unlearning: its nature, scope, and importance for a “delete culture” », *Philosophy & Technology*.

13 Parmi les fondements de licéité, à l'article 6, par. 1, point f) figure : « 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 ».

14 Voir : <https://www.agendadigitale.eu/sicurezza/privacy/Chat-GPT-scorza-la-vera-partita-comincia-adesso-per-una-innovazione-sana/>.

traitement des données personnelles utilisées pour le paramétrage de l'algorithme, avant son éventuelle mise en œuvre via un service de *chatbot*. À ce propos on peut renvoyer à la Délibération de la formation restreinte de la CNIL n°SAN-2022-024 du 20 décembre 2022 concernant la société LUSHA SYSTEMS INC., qui rappelle que, selon l'article 3 du RGPD, lorsque le responsable du traitement ne dispose d'aucun établissement dans l'Union européenne, soit le traitement est lié à une offre de biens ou de services aux personnes concernées, soit le traitement est lié au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union. Or, peut-on en déduire que le traitement des données personnelles réalisé pour l'entraînement de l'algorithme échappe au RGPD et que seulement le traitement des données recueillies pour l'inscription au service et pendant les interactions avec le *chatbot* en soit soumis ?¹⁵ Il faut nuancer. Il est vrai que l'entraînement de l'algorithme GPT, réalisé en dehors de l'UE au moyen d'un traitement massif de données personnelles (ou anonymes), échappe, en soi, au champ d'application territorial du RGPD, mais il est tout aussi vrai que, à partir du moment où l'on choisit de fournir un service à des personnes physiques qui se trouvent sur le territoire de l'Union, la production par cet algorithme de réponses concernant ces personnes physiques est qualifiable de traitement de données personnelles. Ce qui fait que, au moins pour respecter le droit à l'oubli et le droit à la rectification reconnus par le RGPD, le fournisseur du service devrait être en mesure de corriger, rétrospectivement, l'algorithme de façon à ce qu'il ne produise pas les résultats indésirables touchant aux personnes physiques dont les données personnelles ont été utilisées pour entraîner l'algorithme.

B. Extension hors UE du droit au déréférencement

La deuxième actualité concerne la portée territoriale du droit au déréférencement : un droit qui découle de l'article 17 du RGPD, dont l'interprétation a été à plusieurs reprises précisée par la Cour de Justice de l'Union Européenne (CJUE) et le CEPD. La Cour de cassation italienne,

15 F. Mattatia, « Peut-on interdire ChatGPT pour non-conformité au RGPD ? », JCP A, avr. 2023.

première sect. civile, avec la décision du 24 novembre 2022 n° 34658, en est arrivée à admettre un droit au déréférencement global, donc au-delà des frontières de l'UE.

Voici l'affaire qui est à l'origine de la question de droit soumise à la Cour de cassation : un ancien cadre d'Eni, chargé de négocier des projets commerciaux en Irak, au Koweït et à Abou Dhabi, après le classement d'une affaire dans laquelle il avait été impliqué, avait demandé à l'autorité de contrôle italienne d'imposer à Google un déréférencement global des nouvelles le concernant, étant donné qu'il était désormais basé à Dubaï et qu'il opérait professionnellement en dehors de l'Europe. En 2017, l'autorité de contrôle avait ordonné à Google d'étendre ce déréférencement aux versions extra européennes du moteur de recherche, après avoir constaté que Google n'avait supprimé que les résultats des versions européennes de son moteur de recherche.

La Haute juridiction rappelle que d'après la CJUE (arrêt du 24 septembre 2019, Google LLC c. CNIL, C-507/17) le droit de l'Union n'oblige l'exploitant qu'à opérer le déréférencement sur les versions de son moteur correspondant à l'ensemble des États membres, mais les autorités des États membres demeurent compétentes pour effectuer une mise en balance entre, d'une part, le droit de la personne concernée au respect de sa vie privée et à la protection des données à caractère personnel la concernant et, d'autre part, le droit à la liberté d'information, et, au terme de cette mise en balance, pour enjoindre, le cas échéant, à l'exploitant de ce moteur de recherche de procéder à un déréférencement portant sur l'ensemble des versions dudit moteur.

La Cour de cassation observe que, compte tenu du caractère liquide et omniprésent de la circulation des données sur la toile, une limitation, par principe, du droit au déréférencement aux seules versions européennes des moteurs de recherche n'est pas acceptable. Bien qu'un arbitrage entre le droit à l'oubli et le droit à la liberté d'information soit toujours incontournable, les critères pour y procéder ne peuvent que découler du droit européen et national. Peu importe si dans certains pays extra-européens est en vigueur un cadre juridique moins protecteur des droits de la personnalité. Cela ne pourrait que conduire à la non-reconnaissance

de la décision italienne ou à des difficultés d'exécution de la mesure, mais il s'agit de plans distincts : celui de la portée extraterritoriale potentielle des règles et mesures nationales, d'une part ; celui de leur reconnaissance par des États étrangers dans l'exercice de leur souveraineté, d'autre part. Cette souveraineté, explique la Cour, n'est pas compromise par l'efficacité extraterritoriale de la mesure de l'autorité de contrôle nationale, car l'État étranger demeure libre de ne pas reconnaître la mesure ou la décision juridictionnelle qui l'a validée¹⁶.

II. Droit de l'administration électronique

Concernant tout particulièrement la diffusion de solutions d'intelligence artificielle dans l'administration publique, deux actualités méritent d'être signalées : la première touchant au cadre juridique et la deuxième touchant à sa mise en œuvre.

A. Codification dans le Code des contrats publics de la jurisprudence du Conseil d'Etat sur l'emploi d'algorithmes d'IA dans l'action publique.

La première actualité concerne la refonte du Code des contrats publics : le nouveau Code, le décret législatif n° 36 de 2023, est entré en vigueur le 1er avril dernier, mais ses dispositions prennent effet à compter du 1er juillet 2023.

Le 30 juin 2022 le gouvernement a confié au Conseil d'Etat l'élaboration du projet de Code des contrats publics, conformément à la loi n° 78 du 21 juin 2022. Cela a été l'occasion pour le Conseil d'Etat de cristalliser dans l'article 30 du nouveau Code les règles sur la légalité algorithmique, telles que lui-même les avait illustrées notamment avec les décisions n° 2270 du 8 avril 2019 et n° 8472 du 13 décembre 2019.

16 En revanche, le Conseil d'Etat français avait estimé, avec sa décision du 27 mars 2020, n°399922, qu'aucune disposition législative ne prévoit à l'heure actuelle qu'un déréférencement pourrait s'appliquer hors du territoire de l'Union Européenne.

Pour comprendre la portée de cette nouveauté, une petite digression s'avère éclairante.

En Italie, le législateur n'a pas encadré l'emploi d'algorithmes dans le processus décisionnel public (comme ça a été le cas en France avec le Code des relations entre le public et l'administration) et n'a pas utilisé la marge de manœuvre laissée par le RGPD, qui permet aux États membres d'autoriser sous certaines conditions l'adoption de décisions fondées uniquement sur le traitement automatisé de données à caractère personnel (comme ça a été le cas en France avec la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés). Par conséquent, en Italie le recours aux algorithmes d'aide à la décision publique ou la prise automatique d'une décision publique n'étaient soumis qu'au RGPD. Le juge administratif, depuis 2017, a essayé de guider les administrations au biais de multiples décisions, dont les décisions susmentionnées occupent une place de choix. Or, bien que la jurisprudence administrative ait éclairé les retombées du RGPD sur l'algorithmisation de l'action publique, son apport s'arrêtait là : si l'automatisation du processus décisionnel public ne comporte pas un traitement de données personnelles, le RGPD ne s'applique pas et on ne peut que faire confiance au droit commun (notamment le d.lgs. n° 82 de 2005 – Code de l'administration numérique – et à la loi n° 241 de 1990 – la loi fondamentale sur la procédure administrative non contentieuse), qui, malheureusement, se concentre sur la forme numérique de l'acte en laissant de côté la formation électronique de son contenu décisionnel.

Cela dit, la valeur ajoutée de la codification de la jurisprudence du Conseil d'Etat sur les algorithmes publics, même si dans un droit sectoriel, consiste à ce que ce paradigme de « légalité algorithmique » va s'imposer à toute sorte d'automatisation, intégrale ou partielle, du processus décisionnel public, sans considération du caractère personnel ou non personnel des données traitées.

Le nouvel article 30 du Code des contrats publics, portant « utilisation de procédures automatisées dans le cycle de vie des contrats publics », dispose :

- I. Afin d'améliorer l'efficacité, les pouvoirs adjudicateurs automatisent, dans la mesure du possible, leurs activités en utilisant des solutions technologiques, y compris l'intelligence artificielle et les technologies des registres distribués, dans le respect des dispositions spécifiques pertinentes.
- II. Lors de l'acquisition ou du développement des solutions visées à l'alinéa 1, les pouvoirs adjudicateurs :
 - a. assurent la disponibilité du code source, de la documentation et de tout autre élément utile à la compréhension de leur logique de fonctionnement ;
 - b. introduisent des clauses dans l'appel d'offres pour assurer les services d'assistance et de maintenance nécessaires pour la correction des erreurs et des effets indésirables résultant de l'automatisation.
- III. Les décisions prises par l'automatisation doivent respecter les principes de :
 - a. connaissance et intelligibilité, de sorte que tout opérateur économique ait le droit de connaître l'existence de processus décisionnels automatisés le concernant et, le cas échéant, de recevoir des informations significatives sur la logique utilisée ;
 - b. non-exclusivité de la décision algorithmique, ce qui fait que, en tout état de cause, il existe dans le processus décisionnel une contribution humaine capable de contrôler, valider ou réfuter la décision automatisée ;
 - c. non-discrimination algorithmique, consistant à ce que le responsable du traitement mette en œuvre des mesures techniques et organisationnelles appropriées afin d'éviter des effets discriminatoires pour les opérateurs économiques.

- IV. Les pouvoirs adjudicateurs prennent toutes les mesures techniques et organisationnelles appropriées pour garantir que les facteurs conduisant à des données inexactes soient rectifiés et que le risque d'erreurs soit réduit au minimum, et pour prévenir toute discrimination à l'encontre de personnes en raison de leur nationalité, de leur origine ethnique, de leurs opinions politiques, de leur religion, de leurs convictions, de leur appartenance à un syndicat, de leurs caractéristiques somatiques, de leur statut génétique, de leur état de santé, de leur sexe ou de leur orientation sexuelle.
- V. Les administrations publiques publient sur le site institutionnel, dans la section "Administration transparente", la liste des solutions technologiques visées à l'alinéa 1 utilisées pour l'exercice des activités.

B. Expérimentations de l'intelligence artificielle pour orienter l'action publique

La deuxième actualité concerne le développement dans l'administration publique italienne d'outils d'intelligence artificielle, notamment pour orienter les missions de contrôle, ce qui n'a été pas sans engendrer des tensions jurisprudentielles.

Compte tenu de l'ampleur des destinataires, des catégories de données traitées et des technologies employées, ces dernières années l'autorité nationale de contrôle s'est concentrée à plusieurs reprises sur les activités menées par l'administration fiscale et par l'Institut national de la prévoyance sociale (INPS).

Quant à l'administration fiscale italienne, elle vient de développer un outil visant à contribuer à l'analyse du risque d'évasion. Prévu par la loi de finances pour 2020¹⁷ et par un décret du Ministre de l'économie du 28 juin 2022, cet outil (appelé « Vera » - vérification des rapports financiers) permet de recouper les données des contribuables de dizaines de bases de

¹⁷ Article 1, alinéa 681 à 686 de la loi 160 du 27 décembre 2019.

données de l'administration publique et s'appuie aussi sur des techniques de moissonnage de données, pour extraire automatiquement des données structurées et non structurées de sites de la toile¹⁸. L'outil établit ainsi des listes de contribuables à risque qui orientent les activités de contrôle menées par les directions régionales et provinciales. Les critères de fonctionnement ont été présentés par la circulaire n° 21/e du 20 juin 2022¹⁹, même si les détails et l'arbitrage avec le RGPD ont été dévoilés par l'autorité nationale de contrôle, qui a publié son avis favorable à l'analyse d'impact effectuée par l'administration fiscale, conformément à l'article 35 du RGPD²⁰.

Alors que l'outil de l'administration fiscale a été enfin validé par l'autorité de contrôle, ça n'a été pas le cas de l'application mise en œuvre par l'INPS.

De février 2011 à mars 2018 l'INPS a utilisé un logiciel d'analyse de données appelé SAVIO pour gérer les demandes de prestations de maladie et les contrôles médicaux. Le programme informatique attribuait à chaque demande un indice, ou score, lié à certaines variables telles que le pronostic, le lieu d'origine du certificat médical, le nombre de certificats présentés par le travailleur, le secteur de production, l'âge, le sexe, la qualification, le salaire, la taille de l'entreprise et le type de rapport de travail, en comparant les informations contenues dans les certificats avec les informations contenues dans les archives administratives de l'Institut. De cette manière, les demandes étaient associées à un indice relatif à la probabilité de fraudes sur le diagnostic ou le pronostic, ce qui permettait à l'Institut d'orienter les contrôles à domicile. Avec la délibération n° 492 du 29 novembre 2018, l'autorité de contrôle avait infligé une amende administrative de 40000 euros à l'INPS²¹, considérant qu'il avait traité illicitement les données de presque 13 millions de travailleurs privés. Ce sont deux les points contestés par l'autorité de contrôle qui méritent

18 M. Conigliaro, « Lotta all'evasione con l'intelligenza artificiale "VE.R.A." », Fisco, 2022.

19 Voir : https://www.agenziaentrate.gov.it/portale/documents/20143/4495900/Circolare_21_20_06_2022.pdf/5e6b7425-2f02-2b59-480f-c33d9795924e.

20 Voir : <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9808839>.

21 Voir : <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9078812>.

attention, en ce qu'ils ont été validés dans un premier temps par le Tribunal de Rome avec l'arrêt n° 4609 du 3 mars 2020, mais ils viennent d'être définitivement remis en cause par la Cour de cassation.

D'après l'autorité de contrôle et le Tribunal de Rome, le traitement automatisé des données personnelles (y compris « sensibles ») à l'aide du logiciel SAVIO : 1) ne pouvait pas bénéficier des fondements de licéité consistant en le respect d'une obligation légale ou en l'exécution d'une mission d'intérêt public, car le cadre juridique qui établit les missions de contrôle de l'Institut ne prévoit rien quant au type de données et d'opérations qui peuvent être effectuées dans le cadre du traitement automatisé en cause. En d'autres termes, le recours au logiciel SAVIO n'était ni imposé par la loi ni indispensable à l'accomplissement des missions de l'Institut. Il s'ensuit que l'INPS aurait dû recueillir le consentement des personnes concernées ; 2) est qualifiable de profilage et, sous l'empire de l'ancien Code sur la protection des données personnelles (d.lgs. n° 196 de 2003), aurait nécessité une autorisation préalable²².

La Cour de cassation italienne, première sect. civile, avec la décision du 1 mars 2023 n° 6177, casse sans renvoi l'arrêt du tribunal et statue sur le fond, en faisant droit à une partie des moyens soulevés par l'INPS. Ce faisant, la Haute juridiction s'attarde sur le « droit des algorithmes publics » et sur ses coordonnées législatives et jurisprudentielles fondamentales²³.

La Cour observe que :

« avec la décision du 20 mai 2015, n° 10280, elle avait déjà constaté que le droit d'exiger un traitement adéquat de ses données personnelles, bien que relevant des droits fondamentaux de l'article 2 de la Constitution, n'est pas un " tyran " ou un " totem ", exigeant que d'autres droits tout aussi constitutionnellement protégés soient toujours sacrifiés : au contraire, les règles relatives à la protection des données sensibles doivent être coordonnées avec les dispositions constitutionnelles protégeant d'autres droits prépondérants, comme c'est le cas de l'intérêt public à la rapidité, à la transparence et à l'efficacité de l'activité administrative [...] Dans les activités de traitement des données

22 Aujourd'hui, au sens de l'article 35 du RGPD, ce genre de traitement devrait être précédé d'une analyse d'impact, à l'instar du logiciel de l'administration fiscale susmentionné.

23 Cfr. notamment les paragraphes 8 et 9.

à caractère personnel, on peut distinguer deux types de processus décisionnels automatisés : ceux qui impliquent une participation humaine et ceux qui, au contraire, confient l'ensemble du processus à l'algorithme [...] En l'espèce, il ne s'agit pas d'un traitement "purement" automatisé, puisque les opérateurs ont effectué des contrôles supplémentaires, selon des paramètres suggérés par le système [...] Or, le recours à des systèmes informatiques dans l'accomplissement des missions de service public est désormais incontournable dans notre système juridique aussi». A ce sujet, la Cour renvoie aux conclusions de l'avocat général M. G. Pitruzzella, présentées le 27 janvier 2022, dans l'affaire Ligue des droits humains contre Conseil des ministres (CJUE, gde ch., 21 juin 2022, aff. C-817/19, Ligue des droits humains ASBL c/ Conseil des ministres)²⁴, qui estime que ces phénomènes : « s'inscrivent dans le cadre de l'un des principaux dilemmes du constitutionnalisme libéral démocratique contemporain : comment convient-il de définir l'équilibre entre l'individu et la collectivité à l'ère des données, lorsque les technologies numériques ont permis la collecte, la conservation, le traitement et l'analyse d'énormes masses de données à caractère personnel à des fins prédictives ? Les algorithmes, l'analyse des big data et l'intelligence artificielle utilisés par les autorités publiques peuvent servir à promouvoir et à protéger les intérêts fondamentaux de la société, avec une efficacité autrefois inimaginable : de la protection de la santé publique à la durabilité environnementale, de la lutte contre le terrorisme à la prévention de la criminalité, en particulier la criminalité grave [Or, on sait que] le constitutionnalisme européen – national et supranational – avec la place centrale accordée à l'individu et à ses libertés, met une barrière importante à l'avènement d'une société de la surveillance de masse, surtout après la reconnaissance des droits fondamentaux à la protection de la vie privée et à la protection des données à caractère personnel. Dans quelle mesure, cependant, cette barrière peut-elle être érigée sans porter gravement atteinte à certains intérêts fondamentaux de la société – tels que ceux précédemment cités à titre d'exemple – qui peuvent pourtant avoir des liens constitutionnels ? ».

La Cour de cassation rappelle que la jurisprudence administrative, avec notamment les célèbres décisions d'avril et de décembre 2019, a déjà validé, sous certaines conditions, même l'automatisation intégrale de la décision administrative, y compris l'exercice du pouvoir discrétionnaire.

24

Voir :

<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:62019CC0817>.<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:62019CC0817>

Ainsi, d'après la Cour, le recours à des logiciels tels que SAVIO est qualifiable d'exercice du pouvoir d'auto-organisation du service public qui, en plus d'être légitime, s'impose à l'heure numérique, conformément aux principes découlant de la Constitution (art. 97) et des textes organisant la dématérialisation de l'action publique.

Quant à la qualification de profilage, la Cour observe que le logiciel ne classait pas les travailleurs-personnes physiques selon de profils, mais seulement les demandes de prestations de sécurité sociale ; ainsi, dans ce système, il était tout à fait possible que plusieurs demandes, déposées par le même travailleur, avaient des indices différents : ce qui confirme que ce n'étaient pas les travailleurs, mais les demandes de prestations de sécurité sociale qui faisaient l'objet de l'analyse. Sur la base du classement établi par le logiciel, le médecin désigné décidait ensuite des contrôles à effectuer. La Cour remarque que, selon le cadre juridique en vigueur aujourd'hui aussi comme le droit applicable *ratione temporis*, le profilage nécessite : comme étape préliminaire, une activité de préparation et de prédétermination des profils et des catégories, de sorte que les caractéristiques communes des personnes physiques soient identifiées pour chacune d'entre elles ; comme étape exécutive, l'application ultérieure d'un profil, ainsi conçu, à une personne physique. Il s'ensuit que le traitement de données personnelles réalisé par le logiciel SAVIO n'est pas qualifiable de profilage.