Nécessité d'un algorithme transparent pour un consentement valable

Eva Cellina, le 31 août 2021

Le 25 mai 2021, la Cour de cassation italienne a jugé que la logique derrière un algorithme devait être connue par la personne concernée afin qu'elle puisse valablement consentir au traitement de ses données personnelles.

Corte di Cassazione, sez. I Civ. – 25/05/2021, n. 14381

Cette affaire fait suite à une décision de l'autorité italienne de protection des données (GPDP ou Garante) intervenue avant l'entrée en force du RGPD, le 24 novembre 2016.

En bref, l'association Mevaluate Onlus avait alors comme projet de créer un site web visant à l'élaboration de profils réputationnels de personnes physiques et morales inscrites sur la plateforme. Le processus d'évaluation des personnes intéressées devait commencer par le chargement volontaire sur la plateforme, par les utilisateurs, de documents contenant des informations considérées comme importantes en termes de réputation, notamment des documents contenant des informations pénales et fiscales, mais aussi des informations relatives au travail, aux études et à la formation des personnes concernées. Les éléments chargés sur la plateforme par les utilisateurs devaient être d'abord évalués par des consultants spécialisés en profils réputationnels afin de garantir leur authenticité et fiabilité. À la fin des opérations de vérification, le système devait calculer, au moyen d'un algorithme mathématique sophistiqué, une note globale à attribuer aux parties intéressées (dite « note de réputation ») afin de déterminer leur degré de fiabilité. Le score devait ensuite être mis à disposition des autres utilisateurs de la plateforme.

Le Garante estime que le traitement de données effectué par l'association Mevaluate Onlus porte atteinte à la personnalité des personnes concernées. Le traitement de données personnelles se fait sur une base volontaire, dans la mesure où les personnes concernées décident de s'inscrire sur la plateforme et chargent elles-mêmes les documents permettant d'évaluer leur caractère réputationnel. Le traitement se base donc sur le consentement des personnes concernées (art. 7 let. a Directive 95/46/CE). Or, le Garante considère que ce dernier ne peut être valablement donné car il est fourni par crainte d'éventuelles conséquences négatives pour les personnes concernées (manquer la conclusion d'un contrat ou la fin d'une relation

contractuelle). De plus, le Garante relève le nombre élevé de personnes impliquées, l'absence de mesures de sécurité adéquates, le manque de nécessité et de proportionnalité et le manque de fiabilité et d'exactitude du système.

Par conséquent, le Garante a interdit à l'association Mevaluate Onlus de poursuivre le traitement de données personnelles.

Cette décision a fait l'objet d'un recours devant la Cour d'appel civile de Rome, qui, dans sa décision du 4 avril 2018, a partiellement admis le recours en considérant que le traitement des données personnelles en cause était licite, dans la mesure où les personnes concernées avaient consenti à de tels traitements.

Le Garante a ensuite recouru contre cette décision auprès de la Cour de cassation italienne, qui a annulé la décision de la Cour d'appel civile de Rome et ordonné une nouvelle décision.

Ordonnance de la Cour de cassation

Dans son ordonnance du 25 mai 2021, la Cour de cassation italienne considère que les mécanismes de notation et de certification par des personnes privées sont largement connus et répandus. Le traitement des données personnelles des membres de la plateforme Mevaluate Onlus basé sur le consentement des personnes concernées est licite car il est l'expression de l'autonomie privée.

La Cour de cassation confirme la possibilité de développer des services de profils réputationnels basés sur le consentement des personnes concernées à la condition que ce dernier soit valablement donné et qu'il soit exprimé de manière libre et spécifique en référence à un traitement clairement identifié.

La Cour de cassation ajoute ce qui suit :

> « dans le cas d'une plateforme web (avec archives informatiques annexées) destinée à traiter les profils réputationnels de personnes physiques et morales, centrée sur un système de calcul basé sur un algorithme visant à établir des scores de fiabilité, l'exigence de connaissance de la logique derrière l'algorithme ne peut être considérée comme satisfaite lorsque le schéma de mise en œuvre de l'algorithme et les éléments qui le composent restent inconnus ou ne peuvent être connus des personnes concernées » (traduction libre).

L'ordonnance de la Cour de cassation admet ainsi, en principe, la licéité de telles plateformes d'évaluation automatisées de profils réputationnels, à condition de respecter les conditions de validité du consentement énoncées ci-dessus, contrairement au GPDP qui s'y était opposé.

De son côté, l'association Mevaluate Onlus se considère déjà en adéquation avec les exigences de la Cour de cassation, dans la mesure où elle estime avoir indiqué de manière adéquate les critères de fonctionnement de l'algorithme. En effet, tant dans le règlement de l'association que dans le contrat entre chaque membre et le consultant spécialisé en profils réputationnels (chargé de vérifier et certifier l'authenticité des documents déterminants pour procéder à l'évaluation) traitent de la question. Pour ce point, la Cour de cassation a demandé un complément d'instruction à la Cour d'appel civile de Rome qui devra se prononcer dans une nouvelle décision.

Il sera intéressant de voir comment la Cour d'appel civile de Rome va déterminer le caractère transparent de l'algorithme, notamment quant à la question de savoir si une notice d'information ou une clause contractuelle est suffisante pour admettre qu'une personne lambda (sans connaissances particulières en la matière) a été informée des éléments essentiels qui caractérisent l'algorithme et a été capable de les comprendre.

Le RGPD, qui n'est pas applicable à cette affaire, prévoit des règles spécifiques concernant les décisions automatisées. L'art. 22 par. 1 RGPD précise qu'une décision automatisée est une décision fondée exclusivement sur un traitement automatisé de données, produisant des effets juridiques ou affectant de manière significative la personne concernée. Une personne peut notamment faire l'objet d'une décision entièrement automatisée, lorsque la décision est fondée sur le consentement explicite des personnes concernées. L'art. 13 par. 2 let. f RGPD prévoit qu'en cas de décision automatisée, le responsable du traitement informe la personne concernée de l'existence d'une telle décision, ainsi que les informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

En droit suisse, les décisions individuelles automatisées sont celles basées sur un traitement de données personnelles automatisées qui a des effets juridiques ou affectent de manière significative les personnes concernées (art. 21 al. 1 nLPD). Le responsable du traitement a un devoir d'information envers les personnes concernées, à moins que la décision ne soit en relation directe avec la conclusion ou l'exécution d'un contrat (art. 21 al. 3 let. a nLPD) ou que la personne concernée a expressément consenti à la prise de décision automatisée (art. 21 al.

3 let. b nLPD) (voir aussi : Florent Thouvenin/Alfred Früh/Damian George, Datenschutz und automatisierte Entscheidungen, in : Jusletter 26. November 2018).

L'art. 25 al. 2 let. f nLPD prévoit, sur demande de la personne concernée, un droit d'accès de cette dernière à l'existence d'une décision individuelle automatisée la concernant, ainsi qu'à la logique sur laquelle se base la décision. Le Message précise néanmoins qu'il n'y a pas lieu de révéler les algorithmes utilisés, qui relèvent souvent du secret d'affaires, mais plutôt les hypothèses de base qui sous-tendent la logique algorithmique sur laquelle repose la décision individuelle automatisée (FF 2017 6684).

Il est intéressant de constater qu'au sens du RGPD, la personne concernée a un droit d'information s'agissant de la logique sous-jacente à la décision individuelle automatisée, même si elle a consenti à un tel traitement de ses données personnelles (art. 13 par. 2 let. f RGPD). En revanche, au sens de la nLPD, lorsque la personne concernée a consenti à un tel traitement de données, le responsable de traitement n'a pas l'obligation de l'informer activement, mais la personne concernée peut faire valoir son droit d'accès afin d'obtenir des informations, notamment concernant la logique sur laquelle se fonde la décision (art. 21 al. 3 let. a nLPD et art. 25 al. 2 let. f nLPD).

Dans cette affaire, les informations à disposition ne permettent pas de déterminer si la décision peut être considérée comme entièrement automatisée de par l'intervention des consultants spécialisés en profils réputationnels afin de vérifier chaque document transmis par les personnes concernées. Le cas échéant, et à condition que les personnes concernées aient consenti explicitement à une telle décision individuelle automatisée, le traitement pourrait être considéré comme conforme au RGPD et à la LPD. Les principes généraux restent tout de même applicables et pourraient venir limiter un tel traitement.

Proposition de citation : Eva Cellina, Nécessité d'un algorithme transparent pour un consentement valable, 31 août 2021 *in* www.swissprivacy.law/88