# Un arrêt de la Cour de justice de l'UE met en péril les algorithmes de « scoring »

*Théophane Hartmann*

La Cour de justice de l'Union européenne (CJUE) a jugé, jeudi 7 décembre, que toute prise de décision qui utilise des systèmes de notation au moyen de données personnelles est illégale. Cet arrêt pourrait avoir des répercussions importantes pour les caisses de sécurité sociale et les établissements de crédit.

Des années après l'entrée en vigueur du Règlement général de protection des données (RGPD), la Cour de justice de l'Union européenne (CJUE) a rendu son premier arrêt sur l'article relatif à la prise de décision individuelle automatisée.

« Cette décision de la CJUE clarifie le fait que le RGPD contient une interdiction de soumettre les personnes à une prise de décision automatisée ayant un impact significatif sur elles », a expliqué à Euractiv Gabriela Zanfir-Fortuna, vice-présidente protection de la vie privée au Future of Privacy Forum.

Entre 2018 et 2021, un scandale s'est emparé des Pays-Bas – qui a conduit à la démission du troisième gouvernement de Mark Rutte – à propos d'un algorithme de notation défectueux dont l'utilisation a conduit les autorités fiscales à accuser à tort des milliers de personnes d'avoir fraudé un régime de prestations de garde d'enfants.

Jeudi, la Cour a statué que tout type de notation automatisée est interdit s'il a un impact significatif sur la vie des personnes. Le verdict concerne la SCHUFA, la plus grande agence de crédit privée d'Allemagne, qui attribue une note aux personnes en fonction de leur solvabilité.

Selon le jugement, le « *scoring* » de la SCHUFA est en infraction du GDPR si les clients de la SCHUFA – tels que les banques – lui attribuent un rôle « *décisif* » dans leurs décisions contractuelles.

Cette décision pourrait avoir des conséquences importantes. En France, la Caisse nationale des allocations familiales (CNAF) utilise depuis 2010 un algorithme automatisé de « *scoring* » des risques en fonction duquel sont déclenchés des contrôles à domicile pour suspicion de fraude.

*Le Monde* et *Lighthouse Reports* ont rapporté que l'algorithme de « *data mining* » de la CNAF analyse et note 13,8 millions de ménages chaque mois afin de prioriser les contrôles.

L'algorithme de la CNAF utilise une quarantaine de critères basés sur des données personnelles auxquels un coefficient de risque est attribué, notant tous les bénéficiaires entre 0 et 1 chaque mois. Plus le score final des bénéficiaires est proche de 1, plus ils ont de chances de recevoir une inspection à domicile.

Bastien Le Querrec, juriste à La Quadrature du Net, a déclaré à Euractiv : « *Le fait que la CNAF utilise un score automatique pour tous ses allocataires, et, au regard de l'importance prépondérante de ce score dans la suite du processus, ce score a, au sens de* La Quadrature du Net*, des incidences importantes sur la vie des personnes et donc devrait rentrer dans le cadre de la décision de la CJUE, c'est-à-dire être interdit, à moins qu'une loi française l'y autorise, dans le respect strict du RGPD* ».

En d'autres termes, le système de « *scoring* » serait illégal s'il n'était pas spécifiquement autorisé par la loi française et s'il n'était pas strictement conforme aux règles de l'UE en matière de protection des données.

Philippe Latombe, député centriste français (MoDem) et membre de la CNIL, a déclaré à Euractiv qu'il voyait l'algorithme de la CNAF comme un système d'évaluation des risques, filtrant les personnes sur la base de leurs données, qui se trouvent être des données personnelles, du fait de l'objectif de l'organisation : délivrer des allocations aux personnes dans le besoin.

« *Si chaque critère pris séparément peut sembler logique pour lutter contre la fraude, la somme des critères peut être discriminatoire s'ils sont corrélés* », a poursuivi M. Latombe.

Le député écologiste Aurélien Taché a commenté : « *Comme d'habitude, [le gouvernement] combat les pauvres plutôt que la pauvreté, et avec le «* scoring *» social, il ne respecte même plus les principes les plus élémentaires en matière de défense des libertés et de droit à la vie privée* ».

## Restrictions des algorithmes de « *scoring* »

Le RGPD n'autorise les organisations publiques et privées à utiliser des algorithmes de « *data mining* » que dans trois cas : un consentement explicite des individus, une nécessité contractuelle ou une obligation légale.

Mme Zanfir-Fortuna a expliqué que la décision de la Cour de justice de l'UE supprime l'« *intérêt légitime* » des organisations, comme les intérêts commerciaux des entreprises, en tant que base légale suffisante pour effectuer un « *scoring* » qui utilise des données personnelles.

En outre, si un gouvernement souhaite donner une base juridique aux autorités chargées de l'application de la loi pour l'utilisation des algorithmes de « *scoring* », les lois nationales devront fonder leur légitimité sur les lois de l'UE et la Charte des droits fondamentaux de l'UE.

Ces algorithmes doivent être « *nécessaires dans une société démocratique et répondre au critère de proportionnalité* », a déclaré Mme Zanfir-Fortuna. Par conséquent, nourrir des algorithmes de notation avec des données personnelles est désormais beaucoup plus limité dans l'UE.

## Implications

M. Latombe a déclaré que la situation de la CNAF « *soulevait la question de la transparence algorithmique de ParcoursSup* », le portail gouvernemental français conçu pour attribuer les

places dans les universités françaises et autres formations d'études supérieures.

Le site de *La Quadrature du Net* indique par ailleurs que l'Assurance maladie, l'Assurance vieillesse, les Mutualités Sociales Agricoles et Pôle Emploi, utilisent des algorithmes de « *scoring* » similaires, dont la licéité, au regard de l'affaire judiciaire mentionnée, pourrait désormais être remise en question.

En vertu du règlement européen sur l'IA, la loi européenne à venir la plus importante de réglementation de l'intelligence artificielle, les systèmes d'IA destinés à déterminer l'accès aux services publics seront considérés comme « *à haut risque* » et soumis à un régime strict en termes de gestion des risques et de gouvernance des données.