ASSEMBLÉE NATIONALE

16ème legislature

Question N° : 15157	De **M. Philippe Latombe** (Démocrate (MoDem et Indépendants) - Vendée)	**Question écrite**

Ministère interrogé > Enseignement supérieur et recherche	**Ministère attributaire** > Enseignement supérieur et recherche

Rubrique >numérique	**Tête d'analyse** >Vulnérabilités et manque de transparence de Parcoursup	**Analyse** > Vulnérabilités et manque de transparence de Parcoursup.

Question publiée au JO le : **13/02/2024**
Réponse publiée au JO le : **12/03/2024** page : **1884**

Texte de la question

M. Philippe Latombe appelle l'attention de Mme la ministre de l'enseignement supérieur et de la recherche sur Parcoursup. Saisie par l'association Ouvre-boîte d'une demande d'avis, la Commission d'accès aux documents administratifs (CADA) a émis un avis favorable à la communication du code source de l'application Parcoursup, sous réserve de l'occultation des seuls éléments couverts par le secret des systèmes d'information. La commission considérait que celui-ci ne pouvait couvrir que les fragments du code décrivant techniquement les éléments déployés pour la sécurité de l'infrastructure utilisée, tels que ceux permettant de sécuriser la transmission des données avec les serveurs de l'administration. Elle précisait cependant que cette réserve était, par nature, temporaire et qu'il appartenait à l'administration de se conformer progressivement à l'article L. 311-1 du code des relations entre le public et l'administration (CRPA). Le ministère a fait savoir devant le tribunal administratif qu'il ne partageait pas la position de la CADA, notamment parce que le code source comportait de nombreuses vulnérabilités dont la résolution impliquait la réalisation de travaux dont la durée prévisible s'élevait à plusieurs années. L'association requérante a alors saisi le tribunal administratif de Paris. Statuant sur le recours formé par l'association, ce dernier a rejeté la requête, considérant que la publication en ligne du code source complet de l'application Parcoursup en laisserait apparaître les vulnérabilités et serait ainsi susceptible de porter atteinte à la sécurité des systèmes d'information de l'administration. Reconnaître ainsi ces vulnérabilités constitue un véritable appel d'air, un pousse-au-crime pour les pirates. Le mode de défense adopté par le ministère, à la fois dangereux et anti-démocratique, constitue un précédent regrettable. Les premières alertes sur les défaillances de Parcoursup remontent pourtant à plusieurs années. M. le député, qui a lui-même déjà demandé la publication des algorithmes nationaux et locaux, s'étonne que les problèmes n'aient pas encore été résolus et s'interroge sur la compétence de l'entreprise en charge de ce chantier. Il demande à Mme la ministre quelles mesures sont envisagées afin que soit respectée dans les plus brefs délais l'obligation de transparence voulue par le code des relations entre le public et l'administration, tout en assurant la protection des données hébergées par la plateforme. Il souhaite savoir, notamment, quelles solutions sont prévues en cas d'attaque massive du système.

Texte de la réponse

Les traitements qui sont opérés par Parcoursup et qui ont une incidence sur les décisions d'admission ont déjà donné lieu à une diffusion publique (les éléments du code source qui ont été rendus publics sont disponibles sur le dépôt Framagit du ministère de l'enseignement supérieur et de la recherche à l'adresse suivante :

https://framagit.org/parcoursup/algorithmes-de-parcoursup), au sens du quatrième alinéa de l'article L. 311-2 du code des relations entre le public et l'administration (CRPA), accompagnée tant de la publication du cahier des charges synthétique de Parcoursup que d'une publication descriptive complète des algorithmes. Cette publication du code Parcoursup a été effectuée – tant s'agissant de son périmètre que de sa consistance – en plein accord avec le Comité éthique et scientifique de la plateforme Parcoursup, instance indépendante prévue par la loi et dont les rapports annuels au Parlement comportent des avis et recommandations sur le code informatique publié par le ministère. La publication, effectuée conformément aux dispositions du II de l'article L. 612-3 du code de l'éducation, concerne le code informatique du cœur algorithmique de la plateforme Parcoursup, lequel permet à chacun de vérifier que le fonctionnement de la plateforme est conforme au droit et de comprendre les mécanismes de la nouvelle procédure d'entrée dans l'enseignement supérieur : non-hiérarchisation des vœux ; délais de réponses qui permettent, lorsque chaque candidat a fait son choix, de libérer des places qui seront immédiatement proposées à d'autres candidats ; prise en compte des pourcentages déterminés par les recteurs (taux minimum de boursiers, taux maximum de candidats hors secteur pour l'admission en filières non sélectives, modalités d'admission pour les places d'hébergement en internat). Les autres éléments de code qui n'ont pas été rendus publics décrivent notamment les interactions entre l'application Parcoursup et les systèmes d'information du ministère chargé de l'éducation nationale, ceux des établissements d'enseignement supérieur et des utilisateurs ainsi que les procédures de sécurité associées. Saisi d'une demande de communication et de publication du code complet de Parcoursup, et donc de ces éléments, le ministère de l'enseignement supérieur et de la recherche n'a pas donné de suite favorable à cette demande faisant valoir l'exception, prévue par la loi, tenant à l'atteinte qui serait portée par cette communication et cette publication à la sécurité des systèmes d'information des administrations de l'éducation nationale et de l'enseignement supérieur, protégée par le d) du 2° de l'article L. 311-5 du CRPA. Cette position du ministère a été tenue en accord avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et les responsables du ministère en charge de la sécurité des systèmes d'information. Elle ne signifie en rien que la plateforme Parcoursup ne dispose pas d'une stratégie de sécurisation, conduite en lien avec l'ANSSI, au titre de sa mission de contrôle des opérateurs de services essentiels de l'État, et donnant lieu à des homologations régulières. Ainsi, des audits de sécurité sont régulièrement menés pour vérifier la sécurité de l'architecture et du code informatique et attestent d'un niveau de sécurité correct, par rapport à l'état de l'art et à des audits effectués sur un périmètre similaire.