

Feuille de route du GPS

Groupe Pistage et Surveillance

Juillet 2025



La protection de la vie privée des usagers de ressources documentaires sous licence souscrites par les universités françaises tarde à devenir un enjeu suffisamment pris en compte par les professionnels de la documentation et les établissements.

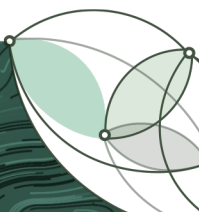
Pour aller au-delà des premiers constats de terrain montrant déjà la forte exposition des données des usagers des plateformes d'édition scientifique, dans le cadre de contrats d'accès souscrits par les services documentaires, trois axes de recherche vont être approfondis pour ce qui concerne spécifiquement le paysage documentaire francophone (Dalloz, Cyberlibris, Europresse, Cairn, etc).

Ces axes de recherche doivent permettre de mieux comprendre les difficultés auxquelles sont confrontés malgré eux les usagers des ressources numériques de l'université dans l'exercice de leurs droits relatifs à la protection de leurs données personnelles.

Premier axe : identifier les mécanismes de pistage à l'œuvre sur les plateformes des éditeurs francophones sur le modèle des analyses déjà fournies par l'organisation SPARC open pour les plateformes Elsevier et Springer

Les dispositifs techniques utilisés par les plateformes des éditeurs scientifiques pour suivre l'activité de leurs utilisateurs peuvent être extrêmement variés, et être tout autant visibles qu'uniquement détectables par des outils d'analyse informatiques. Un premier panorama permet de lister les mécanismes les plus visibles :

- L'incitation forte à créer un compte personnel sur ces plateformes est une première modalité de pistage, très visible : dès l'arrivée sur la plate-forme, malgré l'authentification fournie par le mécanisme d'accès par le proxy de son établissement dans la plupart des cas, l'utilisateur est informé de la nécessité de créer un compte personnel, généralement inutile pour garantir l'accès aux contenus.
- L'utilisation de cookies est évidemment mentionnée : là, une analyse approfondie est à conduire pour mieux apprécier le caractère réellement nécessaire des cookies mentionnés comme tels, sachant que l'exercice du consentement (ou du « dé-consentement ») utilisateur est loin d'être évident.
- Des analyses techniquement plus approfondies permettent rapidement d'identifier la présence de dispositifs (complémentaires ou remplaçant progressivement les cookies tiers) tels que : les traceurs, les outils de prise d'empreintes numériques et ceux d'agrégation de données d'audience. Ces analyses nécessitent d'être poussées pour en dresser un inventaire plus exhaustif.



Deuxième axe : évaluer le degré de protection prévu dans les licences et contrats en vigueur, dans le cadre de négociations nationales menées par le consortium Couperin, suivant en cela le chemin montré par d'autres consortia similaires (DEAL en Allemagne, SURF aux Pays-Bas).

La lecture rapide des contrats pose rapidement plusieurs problèmes liés au renvoi systématique à des politiques de confidentialité propres aux éditeurs, très générales, parfois peu compréhensibles, éventuellement mouvantes et peu protectrices.

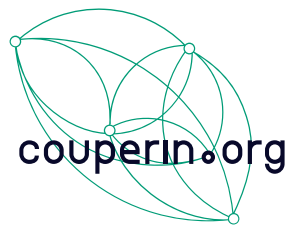
- Une évaluation de ces politiques de confidentialité doit permettre d'identifier les priorités en termes de modifications à apporter aux licences discutées lors des négociations Couperin.
- Ces analyses seront complétées par les questionnaires envoyés aux éditeurs, afin qu'ils détaillent plus précisément leurs pratiques de protection des données.
- Enfin, l'exercice des droits des usagers des ressources numériques sera réellement évalué. Au-delà du contenu des licences, le contrôle de leur mise en application réelle et le respect de la loi est également à tester. Les tentatives d'utilisateurs de ces plateformes pour réclamer leurs données auprès des plateformes sont à multiplier pour comprendre si les premiers résultats – révélateurs d'une énorme défaillance à ce niveau – sont réellement représentatifs d'une situation désastreuse.

Troisième axe : comprendre les raisons du manque d'informations fournies aux usagers par les bibliothèques universitaires françaises et la faiblesse du niveau de prise en compte concernant le respect de la vie privée.

Une enquête à destination des professionnels des bibliothèques universitaires doit permettre de mieux apprécier au sein de la profession :

- Le degré de méconnaissance du fonctionnement des plateformes d'édition scientifique, du point de vue de la protection des données, et permettre d'en identifier les causes, les hypothèses travaillées étant : le faible nombre des effectifs de professionnels dévolus à ces sujets ; le contexte évolutif rapide de la problématique de la protection des données (notamment du point de vue technique).
- Le poids du sentiment que les mécanismes techniques d'accès aux plateformes sont suffisamment protecteurs : quand l'authentification des utilisateurs peut passer par une connexion anonyme via le proxy établissement, quand les bannières de cookies semblent sécuriser et pouvoir limiter au strict nécessaire le consentement des utilisateurs, la vigilance des professionnels semble diminuer vis-à-vis d'autres dispositifs, tout autant si ce n'est plus intrusifs envers la vie privée des usagers des bibliothèques, mais moins visibles.
- Les failles dans l'évaluation du risque encouru par les établissements et les usagers des plateformes d'édition scientifique : l'absence d'alternative pour accéder à des contenus souvent exclusifs, et indispensables pour les chercheurs, semble être une des raisons majeures expliquant le passage à l'arrière-plan les défauts des pratiques





et politiques de confidentialité des éditeurs, ne conduisant encore que trop rarement les établissements à une analyse des risques juridiques et concernant la sécurité des données utilisateurs.

In fine, l'ensemble des angles d'approche doit à terme permettre au consortium Couperin d'activer de manière très opérationnelle les leviers qui permettront que cet enjeu soit mieux pris en compte dans les négociations, dans le but d'offrir un accès plus protecteur pour les usagers, leur permettre a minima un réel exercice de leurs droits et aller si possible au-delà des garanties déjà couvertes par le RGPD.

