Scraping : la Cour suprême américaine remet LinkedIn sur les rails

Quelles méthodes légales pour interdire l'accès à un système informatique ? C'est l'une des questions auxquelles la justice américaine semble devoir répondre dans l'affaire « LinkedIn vs hiQ ».

Au cœur du dossier, le *scraping*, collecte massive et automatisée de données. LinkedIn avait porté le fer contre un de ses pratiquants : hiQ Labs. Cette entreprise exerce toujours son activité d'alors : elle récupère des informations sur les profils publics du réseau social, les met en forme et les commercialise, sous l'angle de l'analyse prédictive. Sa cible : les employeurs soucieux de détecter le personnel qui envisage de mettre les voiles.

LinkedIn avait demandé à hiQ de cesser la pratique, au nom du Computer Fraud and Abuse Act. Cette loi date de 1986. Dans les grandes lignes, elle punit le fait d'accéder à un ordinateur sans permission ou d'utiliser à outrance un accès autorisé.

Face à cette injonction, hiQ avait saisi la justice en Californie pour tenter de prouver que son activité était légale. Et l'avait emporté. C'était en 2017. Deux ans plus tard, LinkedIn, ayant fait appel, était débouté. Entre autres pour les motifs suivants :

- Le réseau social n'a pas de droits sur les données que publient ses membres, ces derniers étant propriétaires de leur profil.
- Les utilisateurs qui choisissent un profil public attendent « évidemment » qu'il soit accessible par des tiers.
- Le Computer Fraud and Abuse Act est censé régir les cas de piratage. Il est d'autant plus discutable de l'invoquer dans une affaire concernant des données en accès libre.
- Laisser à LinkedIn le contrôle sur l'utilisation des données publiques pourrait engendrer un « monopole de l'information » préjudiciable à l'intérêt public.
- Sans accès aux données concernées, hiQ ferait face à des « dommages irréparables ».

Une deuxième chance pour LinkedIn

La procédure était finalement remontée jusqu'à la Cour suprême. Celle-ci vient de se prononcer… et de renvoyer l'affaire en Cour d'appel. En toile de fond, une autre décision, prise début juin. Elle restreint le champ d'application du Computer Fraud and Abuse Act.

> *OPINION: 19-783 Van Buren v. United States https://t.co/OAKwv2gtte*
>
> *An individual "exceeds authorized access" when he accesses a computer with authorization but then obtains information located in particular areas of the computer that are off-limits to him.*
>
> *BARRETT*
>
> *— U.S. Supreme Court (@USSupremeCourt) June 3, 2021*

L'affaire concerne un officier de police qui avait utilisé une base de données gouvernementale pour mener une enquête de sa propre initiative. Le raisonnement de la Cour suprême a été – en résumé – le suivant :

- Au regard du Computer Fraud and Abuse Act, un individu ne peut être tenu responsable que s'il on obtient des informations sur des « zones particulières » d'un système informatique (fichiers, dossiers, bases de données…) auxquelles ses droit d'accès ne s'étendent pas.
- L'officier avait accès à l'information dans le cadre de son travail. Aussi pouvait-il s'en servir peu importe les finalités.

La question des « méthodes légales », elle, reste en suspens. Il s'agit de savoir si ledit raisonnement s'applique en cas d'existence d'une forme de « barrière ». LinkedIn affirme en avoir mis deux en place. D'un côté, sa lettre d'injonction envoyée à hiQ avant d'aller en justice. De l'autre, des mesures « à base de code » sur ses serveurs.

Photo d'illustration © 360b – Shutterstock