_swissprivacy.law

Web scraping de profils publics sur LinkedIn

Pauline Meyer, le 9 juin 2022

LinkedIn doit continuer à accorder à une société d'analyse de données partenaire l'accès aux profils publics de ses utilisateurs.

Decision No. 17–16782 of the United States Court Of Appeals For The Ninth Circuit, 18 avril 2022

Le 18 avril 2022, la Cour d'appel du neuvième circuit de Californie (United States Court Of Appeals For The Ninth Circuit) prononce une injonction préliminaire visant à interdire provisoirement à LinkedIn Corp. de refuser à hiQ Labs Inc., une entreprise d'analyse de données, l'accès aux profils de membres de LinkedIn accessibles au public.

LinkedIn est un site Internet de réseautage professionnel contenant des profils de membres accessibles à tout public. La société dispose de mesures permettant de limiter cet accès et assurer la sécurité des données traitées. Tout d'abord, les membres ont la possibilité de ne pas notifier leur communauté lorsqu'ils effectuent une modification de leur profil. Ensuite, les serveurs de l'entreprise sont protégés des accès non autorisés et leur accès est limité à certaines entités, comme le moteur de recherche Google, qui bénéficient d'une autorisation expresse. Finalement, LinkedIn emploie plusieurs systèmes techniques pour détecter des activités suspectes et restreindre l'extraction automatisée de données.

HiQ, entreprise d'analyse de données, effectue du *web scraping*. Le *web scraping* consiste en l'extraction (ou l'aspiration) et la copie de données provenant d'un site web en un format structuré permettant des analyses. Ce procédé peut être fait manuellement ou de manière automatisée. La société utilise des bots automatisés pour extraire les données contenues dans les profils publics des utilisateurs de LinkedIn, ensuite traitées par un algorithme prédictif afin de vendre à ses clients commerciaux deux types d'analyses de personnes. L'une permet aux employeurs d'offrir des opportunités de développement de carrière, bonus et autres avantages pour conserver leurs bons employés. La seconde résume les compétences afin de permettre aux employeurs de percevoir des lacunes et mettre en place des formations internes.

La Cour d'appel a rendu une première décision en septembre 2019, en confirmant la décision

du tribunal du district et en permettant à hiQ de continuer à extraire les données des profils publics de LinkedIn. À la suite de sa saisine par LinkedIn, la Cour suprême a ensuite renvoyé l'affaire à la Cour d'appel pour un nouvel examen à la lumière de l'arrêt *Van Buren v. United States* rendu en 2021.

La Cour d'appel indique qu'une injonction préliminaire (*preliminary injucntion*) peut être prononcée si le requérant établit :

1. qu'il est susceptible de réussir sur le fond de l'affaire ;
2. qu'il est susceptible de subir un dommage irréparable en l'absence de cette injonction ;
3. que ses intérêts dans la mise en balance entre les intérêts en présence sont prépondérants ;
4. que la mesure provisionnelle va dans le sens d'un intérêt public.

La Cour d'appel analyse d'abord le critère du dommage irréparable. Elle conclut qu'en raison de l'activité d'hiQ, l'entreprise dans son entier serait compromise si elle ne pouvait plus bénéficier des informations mises à disposition par LinkedIn. Il n'existe en effet pas d'autre base de données publiquement accessibles contenant des données similaires.

Dans l'analyse des intérêts en présence, la Cour d'appel rappelle qu'hiQ, d'une part, est susceptible de faire faillite en l'absence d'une décision allant dans son sens. LinkedIn soulève d'autre part que la sphère privée de ses membres est menacée dans la mesure où un profil public n'équivaut pas au consentement qu'un tiers collecte et utilise ces données à d'autres fins que celles initialement convenues. La Cour relève tout d'abord qu'il est peu probable que les utilisateurs disposant d'un profil public s'attendent à ce que les informations qu'ils publient demeurent privées. Qui plus est, la politique de confidentialité de LinkedIn conseille de ne pas partager de données personnelles qui seraient par conséquent accessibles au grand public. Ensuite, il n'existe pas de preuve que les utilisateurs choisissant le paramètre ne notifiant pas leur communauté en cas d'ajout ou modification d'informations procèdent à ce choix afin de ne pas rendre leurs données (toujours accessibles sur leur profil) publiques. Il peut s'agir d'éviter d'ennuyer ses connexions avec des notifications ou d'éviter d'alerter son employeur de modifications précédant une recherche d'emploi. Finalement, les actions de LinkedIn vont dans le sens opposé d'une préservation de la sphère privée, l'entreprise offrant des produits permettant par exemple aux recruteurs d'être alertés par certaines informations. Pour toutes ces raisons, la Cour d'appel conclut que les intérêts privés de hiQ priment ceux invoqués par LinkedIn.

La Cour estime qu'hiQ a des chances de succès sur le fond, en se basant sur une potentielle

ingérence délictueuse de LinkedIn dans les contrats d'hiQ avec des tiers (*tortious interference with contract*) et sur les règles relatives aux accès non autorisés à un système informatique selon le *Computer Fraud and Abuse Act* (CFAA, 18 U.S.C. § 1030).

La Cour estime finalement que l'intérêt public défendu par hiQ prime celui de LinkedIn. La volonté de ne pas attribuer trop de pouvoir à des plateformes comme LinkedIn prime le fait que le *web scraping* puisse potentiellement inciter des acteurs malveillants à accéder aux données de LinkedIn.

Pour ces motifs, la Cour d'appel confirme la décision du tribunal de district. Elle confirme qu'hiQ a établi les éléments requis et renvoie l'affaire à l'instance inférieure.

En droit suisse de la protection des données personnelles, la nouvelle LPD introduit la notion de « violation de la sécurité des données » (art. 5 let. h nLPD). Selon nous, l'aspiration ou l'extraction par un bot automatisé d'une multitude de données librement accessibles ne constitue pas une telle violation, les données étant précisément librement accessibles. En outre, nous estimons que, selon le nouveau droit suisse, il n'y a pas d'atteinte à la personnalité pour ce traitement de données (principalement au regard du principe de finalité), dans la mesure où les données sont rendues librement accessibles au public par la personne concernée et que cette dernière ne s'est pas opposée pas expressément à un tel traitement (art. 30 al. 2 nLPD). Cette question n'a toutefois pas été tranchée à l'heure actuelle. En revanche, les personnes concernées doivent selon nous être informées si un responsable du traitement autorise le *web scraping* de leurs données. En effet, l'art. 19 nLPD (devoir d'information) s'applique également en cas de données rendues librement accessibles par la personne concernée, sous réserve des exceptions usuelles de l'art. 20 nLPD.

À noter que le *web scraping* peut soulever des questions contractuelles, de concurrence, de droit pénal ou de propriété intellectuelle en droit suisse (voir par exemple Florent Thouvenin, Un droit de propriété sur les données en droit suisse ?, in : Jacques de Werra, Propriété intellectuelle à l'ère du Big Data et de la Blockchain, p. 97 s.).

Proposition de citation : Pauline Meyer, Web scraping de profils publics sur LinkedIn, 9 juin 2022 *in* www.swissprivacy.law/150