Exploitation des profils LinkedIn sans consentement

Conseils pratiques publié le **21/03/2025**, vu **649 fois**, Auteur : Murielle Cahen

À l'aube de ce XXIe siècle, une mutation profonde des interactions professionnelles s'est opérée, propulsée par l'essor inéluctable des technologies numériques. et en particulier linkdn.

Les plateformes en ligne, parmi lesquelles LinkedIn occupe une place prépondérante, ont redéfini les mécanismes de mise en relation entre les individus, favorisant une exposition sans précédent des compétences et des expériences professionnelles à une audience mondiale. Cette dynamique soulève des enjeux cruciaux concernant la protection des données personnelles, dont le statut est devenu ambivalent dans un monde où la visibilité professionnelle est souvent synonyme de partage d'informations sensibles.

Le jugement énoncé par le tribunal de commerce de Paris le 30 septembre 2024 s'inscrit dans ce débat contemporain, marquant une avancée significative dans la compréhension des interactions entre utilisateurs et plateformes numériques. En affirmant que l'exploitation des informations disponibles sur des profils publics de LinkedIn n'exige pas le consentement explicite des utilisateurs, conformément aux dispositions de l'article 5 du Règlement général sur la Protection des Données (RGPD), ce verdict interroge la notion même de consentement à l'ère numérique.

Il met en lumière un dilemme central : les utilisateurs, en rendant leurs profils accessibles, semblent accepter tacitement une exploitation potentielle de leurs données personnelles, tout en recherchant activement des opportunités professionnelles. Ce jugement soulève également une série de questions sur la responsabilité partagée entre les utilisateurs et les plateformes. D'un côté, les individus aspirent à se faire connaître, à se démarquer dans un marché du travail compétitif, et à attirer l'attention d'employeurs potentiels. De l'autre, cette quête d'accessibilité les expose à des risques inhérents à une exploitation non régulée de leurs informations.

Ainsi, se dessine un paradoxe : celui d'un partage volontaire qui s'accompagne d'une vulnérabilité face aux pratiques commerciales des tiers. La responsabilité des utilisateurs dans la gestion de leurs données personnelles se trouve dès lors mise en exergue, appelant à une prise de conscience accrue de leurs droits et des enjeux qui en découlent.

En parallèle, la décision judiciaire a révélé que la plateforme poursuivie, bien qu'elle n'ait pas été reconnue en infraction au RGPD, avait violé ses propres conditions générales d'utilisation. En utilisant des profils LinkedIn pour offrir des services à ses clients, elle a franchi une ligne, se rendant coupable de pratiques de concurrence déloyale. Ce constat souligne l'importance cruciale pour les plateformes de respecter les règles qu'elles établissent elles-mêmes afin de protéger les droits des utilisateurs tout en assurant un cadre de concurrence éthique. Il en va de la crédibilité des plateformes et de la confiance que leur accordent les utilisateurs. L'absence de plaintes déposées auprès de la Commission nationale de l'informatique et des libertés (Cnil) met également en lumière une lacune significative en matière de sensibilisation des utilisateurs quant à leurs droits. Ce manque d'information soulève des interrogations sur le rôle des plateformes dans l'éducation des utilisateurs, les exhortant à une vigilance accrue face aux enjeux de la

protection des données.

Les utilisateurs portent une part de responsabilité dans la gestion de leurs informations personnelles ; cependant, il incombe également aux plateformes de fournir les outils et les informations nécessaires pour garantir une utilisation éclairée de leurs services. Il est donc impératif d'engager une réflexion approfondie sur les implications juridiques, éthiques et pratiques liées à l'exploitation des données personnelles sur des réseaux tels que LinkedIn.

Cette analyse doit transcender la simple conformité légale et s'inscrire dans une perspective éthique, où la protection des données personnelles devient un enjeu fondamental de la confiance.

À la croisée des chemins entre droit et éthique, se dessine un futur où la transformation numérique ne doit pas se faire au détriment des droits fondamentaux des individus. En promouvant une culture de la protection des données, nous pouvons espérer bâtir un environnement numérique où les opportunités professionnelles coexistent harmonieusement avec le respect des droits et de la dignité des utilisateurs.

I. Le cadre juridique de l'utilisation des données personnelles sur LinkedIn

A. Les dispositions du RGPD et leur application aux profils publics

Le Règlement Général sur la Protection des Données (RGPD), entré en vigueur le 25 mai 2018, représente une avancée significative dans la protection des données personnelles au sein de l'Union Européenne.

L'article 5 du RGPD établit des principes directeurs qui régissent la collecte et le traitement des données personnelles. Parmi ces principes, on trouve la licéité, la loyauté et la transparence, la limitation des finalités, la minimisation des données, l'exactitude, la limitation de la conservation, et l'intégrité et la confidentialité. Dans le contexte des profils publics sur LinkedIn, la question de la licéité du traitement des données personnelles est primordiale. En effet, les utilisateurs de LinkedIn, en choisissant de rendre leurs profils accessibles au public, consentent implicitement à ce que leurs informations soient utilisées par des tiers, notamment par des recruteurs ou des entreprises.

Selon l'article 6 du RGPD, le traitement des données peut être considéré comme licite lorsque la personne concernée a donné son consentement, lorsque le traitement est nécessaire à l'exécution d'un contrat, ou lorsque le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou un tiers, sauf si prévalent les intérêts ou les droits et libertés fondamentaux de la personne concernée.

Il est également important de noter que l'article 7 du RGPD impose des exigences strictes quant à la manière dont le consentement doit être donné. Ce consentement doit être libre, spécifique, éclairé et univoque. Cependant, dans le cadre des profils publics sur LinkedIn, la question du consentement explicite devient plus complexe.

L'utilisateur, en créant un profil public, pourrait être considéré comme ayant donné son consentement implicite à l'utilisation de ses données. Cela soulève des interrogations sur la portée de ce consentement implicite et sur la responsabilité des plateformes dans l'information des utilisateurs concernant l'utilisation de leurs données.

Un exemple pertinent est celui de la décision de la Cour de Justice de l'Union Européenne (CJUE) dans l'affaire Google Spain SL, Google Inc. c/ Agencia Española de Protección de Datos, Mario Costeja González (C-131/12).

La Cour a jugé que les moteurs de recherche, en tant que responsables du traitement, sont tenus de garantir le droit à l'effacement des données personnelles (droit à l'oubli) lorsque les informations sont inexactes, incomplètes ou non pertinentes. Cette décision illustre l'importance de la transparence et de la responsabilité dans le traitement des données personnelles, des principes qui sont également applicables dans le contexte des réseaux sociaux comme LinkedIn.

B. La notion de consentement implicite et ses implications

La notion de consentement implicite est un sujet de débat majeur dans le domaine de la protection des données personnelles, surtout lorsqu'il s'agit de plateformes en ligne où les utilisateurs partagent volontairement des informations. Dans le cadre des profils publics sur LinkedIn, le consentement implicite peut être interprété comme une acceptation tacite des utilisateurs à ce que leurs données soient utilisées par des tiers, en raison de la nature même de la plateforme, qui vise à faciliter les interactions professionnelles. Cependant, cette interprétation du consentement implicite soulève des questions éthiques et juridiques. Par exemple, il est essentiel de déterminer si les utilisateurs sont réellement conscients des implications de rendre leurs informations accessibles publiquement.

La Cour de cassation française a, dans son arrêt du 26 juin 2019, rappelé que le consentement doit être éclairé et que l'absence d'information claire sur l'utilisation des données peut constituer une violation des droits des personnes concernées.

En outre, la directive européenne 2016/680 relative à la protection des données à caractère personnel traitées dans le cadre des activités policières et judiciaires souligne la nécessité d'un consentement explicite lorsque les données sensibles sont en jeu, comme les informations relatives à la santé ou à l'origine ethnique.

Bien que ces dispositions s'appliquent principalement à d'autres contextes, elles illustrent l'importance d'un consentement clair et éclairé dans le traitement des données personnelles, y compris sur des plateformes professionnelles. Un exemple pratique est celui des utilisateurs qui, en raison de l'interface de LinkedIn, peuvent ne pas réaliser que la sélection de certaines options de visibilité entraîne une exposition de leurs données. La responsabilité incombe donc à la plateforme de veiller à ce que ses utilisateurs soient pleinement informés des conséquences de leurs choix en matière de visibilité. À cet égard, le Règlement impose aux responsables du traitement de fournir des informations claires et compréhensibles sur l'utilisation des données personnelles.

Cela inclut des détails sur la finalité du traitement, la durée de conservation des données et les droits des utilisateurs.

En somme, si le consentement implicite peut être perçu comme suffisant dans certains cas, son application sur des plateformes comme LinkedIn reste délicate. Les utilisateurs doivent être pleinement conscients de l'impact de leurs décisions et de la manière dont leurs données peuvent être utilisées par des tiers.

La transparence et la responsabilité des plateformes sont donc essentielles pour garantir que les droits des utilisateurs soient respectés et que leur consentement soit véritablement éclairé. Il est donc impératif que LinkedIn et d'autres réseaux sociaux clarifient leur politique de protection des données et s'assurent que les utilisateurs comprennent les implications de leur choix de rendre leurs profils publics.

II. La concurrence déloyale et le respect des conditions d'utilisation

A. Les pratiques de web scraping et leurs conséquences juridiques

Le web scraping, ou extraction automatisée de données à partir de sites web, est une pratique qui soulève de nombreux enjeux juridiques, notamment en ce qui concerne le respect des conditions d'utilisation des plateformes. Dans le contexte des réseaux sociaux et des plateformes de recrutement comme LinkedIn, cette pratique peut être perçue comme une violation des droits d'auteur, une atteinte à la protection des données personnelles, et une infraction aux dispositions relatives à la concurrence déloyale.

Sur le plan du les bases de données sont protégées par le Code de la propriété intellectuelle. En France, l'article L. 112-3 dispose que les bases de données sont considérées comme des œuvres de l'esprit, et leur extraction non autorisée peut constituer une atteinte aux droits moraux et patrimoniaux de l'auteur.

L'affaire "LinkedIn c. hiQ Labs" est emblématique de cette problématique. Dans cette affaire, LinkedIn a tenté d'interdire à hiQ Labs, une entreprise de web scraping, d'extraire des données de ses utilisateurs. La Cour d'appel de San Francisco a statué en faveur de hiQ, affirmant que l'accès aux données publiques ne constituait pas en soi une violation des conditions d'utilisation de LinkedIn. Cependant, cette décision a été critiquée pour son manque de clarté quant aux droits des plateformes de contrôler l'accès à leurs données.

En outre, le web scraping peut également être considéré comme une concurrence déloyale, notamment lorsqu'il porte atteinte aux intérêts commerciaux légitimes des plateformes.

L'article 1240 du Code civil dispose que Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer. Dans ce cadre, les entreprises victimes de web scraping peuvent engager des poursuites pour obtenir des réparations.

Par exemple, si une entreprise utilise les données collectées via le scraping pour proposer des services similaires à ceux d'une plateforme, cela peut être interprété comme une exploitation déloyale des efforts d'investissement et de développement de cette dernière.

Les conséquences de telles pratiques ne se limitent pas uniquement aux aspects juridiques ; elles peuvent également avoir un impact significatif sur la concurrence dans le secteur des plateformes de recrutement. L'utilisation abusive des données peut créer un déséquilibre sur le marché, favorisant les acteurs qui recourent à ces pratiques au détriment de ceux qui respectent les conditions d'utilisation. Cela soulève des questions sur l'équité et l'intégrité de la concurrence, en particulier dans un domaine où la confiance des utilisateurs est primordiale.

B. Les enjeux éthiques et la protection des données personnelles

Les enjeux éthiques liés à l'utilisation des données personnelles dans un cadre commercial sont d'une importance capitale, surtout dans un contexte où les utilisateurs partagent de plus en plus d'informations en ligne. Le droit à la vie privée, protégé par le RGPD, impose des obligations strictes aux entreprises concernant la collecte, le traitement et la conservation des données personnelles. Toutefois, l'exploitation des données à des fins commerciales, notamment par le biais du web scraping, pose des défis éthiques majeurs. Il est crucial de trouver un équilibre entre

l'accès à l'information et la protection des droits individuels.

D'un côté, les entreprises ont un intérêt légitime à utiliser les données pour améliorer leurs services et répondre aux besoins des utilisateurs.

De l'autre, les utilisateurs ont le droit d'attendre que leurs données soient traitées de manière responsable et dans le respect de leur vie privée. Les récents scandales liés à la fuite de données personnelles, tels que l'affaire Cambridge Analytica, ont mis en lumière les dangers d'une exploitation non éthique des données, entraînant une perte de confiance des utilisateurs envers les plateformes. Dans ce contexte, il est essentiel d'instaurer des recommandations pour une meilleure régulation des pratiques liées à l'exploitation des données personnelles. Cela pourrait inclure des mesures telles que :

1. Renforcement de la transparence : Les plateformes doivent être tenues de fournir des informations claires et accessibles sur la manière dont les données des utilisateurs sont collectées, utilisées et partagées. Cela inclut la mise à jour régulière des politiques de confidentialité et des conditions d'utilisation.

2. Consentement explicite : Les entreprises doivent obtenir un consentement explicite de la part des utilisateurs avant de procéder à la collecte de leurs données. Ce consentement doit être libre, éclairé et spécifique, conformément aux exigences du RGPD.

3. Responsabilité des plateformes : Les entreprises qui exploitent des données personnelles doivent être responsables de leur utilisation, en veillant à respecter les droits des utilisateurs et à protéger leurs données contre toute utilisation abusive. Cela pourrait inclure l'instauration de mécanismes de contrôle et de vérification pour s'assurer que les données collectées ne sont pas utilisées à des fins contraires à l'éthique ou à la loi.

4. Sanctions dissuasives : Il est impératif que des sanctions adéquates soient mises en place pour décourager les pratiques de web scraping non éthiques. Cela pourrait impliquer à la fois des amendes financières substantielles et des mesures d'interdiction d'accès aux plateformes pour les entreprises qui enfreignent les conditions d'utilisation.

5. Sensibilisation des utilisateurs : Les utilisateurs doivent être mieux informés de leurs droits en matière de protection des données. Cela inclut la compréhension des implications de la publication de leurs informations sur les réseaux sociaux et des mesures qu'ils peuvent prendre pour protéger leur vie privée.

6. Encadrement juridique des pratiques de scraping : Il serait bénéfique d'établir un cadre juridique clair concernant le web scraping, notamment en définissant les situations où cette pratique peut être considérée comme légitime, tout en protégeant les droits des détenteurs de données. Cela pourrait inclure des exemptions pour des usages spécifiques tels que la recherche académique ou l'analyse de données, à condition que cela soit réalisé dans le respect des droits des utilisateurs.

Sources :

1. Legalis | L'actualité du droit des nouvelles technologies | Pas de consentement nécessaire pour utiliser des profils sur LinkedIn

2. CURIA - Documents

3. Cour de cassation, civile, Chambre civile 1, 26 juin 2019, 18-15.830, Publié au bulletin - Légifrance

4. Directive - 2016/680 - EN - règlement bruxelles ii ter - EUR-Lex

5. Web Scraping : Tout ce qu'il faut savoir

6. LinkedIn remporte la dernière bataille judiciaire contre le grattage des données et l'utilisation abusive des informations des utilisateurs - Coeur sur Paris