ALEPH-NETWORKS
75 rue de l'église
69480 POMMIERS

Lyon, le 4 septembre 2025

**Olivier Moussa**
Avocat associé
Spécialiste
propriété intellectuelle
et numérique
Magistère DJCE
Chargé d'enseignement
à l'Université
om@shift-avocats.com

**Gérald Sadde**
Avocat associé
Docteur en droit
gs@shift-avocats.com

**Gaëtan Bourdais**
Avocat associé
gb@shift-avocats.com

**Alexandre Marraud des Grottes**
Avocat collaborateur
amdg@shift-avocats.com

## Consultation juridique sur les services fournis par Aleph

Madame, Monsieur,

Vous nous avez consulté afin que nous répondions aux questions juridiques les plus courantes que votre clientèle se pose s'agissant de votre moteur de recherche Aleph SEARCH comme de votre service Aleph ALERT.

Ces questions sont les suivantes :

1. Est-il licite de consulter le *Dark Web* ou le *Deep Web* ?
2. Le service Aleph SEARCH proposé par Aleph est-il licite ?
3. Le service Aleph ALERT proposé par Aleph est-il licite ?
4. La différence est que les clients d'Aleph ne peuvent consulter que les résultats de mots-clés de recherche préalablement définis.Quel est le statut juridique d'un moteur de recherche en ligne comme celui d'Aleph SEARCH ?
5. Quelle est la responsabilité d'un moteur de recherche comme Aleph SEARCH en cas de référencement d'un contenu illicite ?
6. Pourquoi Aleph ne recherche pas de façon offensive les fuites de données comme d'autres prestataires ?
7. La recherche sur internet de fuite d'informations (RIFI) est-elle licite ?
8. Pourquoi la RIFI nécessite la signature d'un mandat ?

Vous trouverez ci-après notre consultation.

Nous demeurons naturellement à votre disposition pour en discuter et vous prions de croire, Madame, Monsieur, à l'assurance de nos sentiments les meilleurs.

Gérald Sadde Gaëtan Bourdais

**SHIFT avocats**

Immeuble
Sainte-Marie des Terreaux
21 rue d'Algérie
69001 Lyon - France

T +33 (0)478 928 928
F +33 (0)472 618 208
W www.shift-avocats.com
Toque n° 194

Avocats au barreau de Lyon
SELARL au capital de 100 000 €
RCS Lyon 443 732 268
APE 6910Z

## 1. Est-il licite de consulter le *Dark Web* ou le *Deep Web* ?

Oui, il est licite de consulter le *Dark Web* ou le *Deep Web*.

Ces termes ne correspondent à aucune notion juridique existante en droit français ou européen.

- Le ***Deep Web*** désigne les sites internet qui ne sont pas indexés par les moteurs de recherche généralistes (Google, Bing, etc.).

  Plusieurs raisons peuvent l'expliquer : algorithme du moteur de recherche ne jugeant pas le contenu pertinent, éditeur du site ne souhaitant pas être référencé, contenu uniquement accessible avec un compte utilisateur, etc.

- Le ***Dark Web*** désigne les sites internet qui sont accessibles uniquement par l'intermédiaire de protocoles spécifiques ou de réseaux d'anonymisation.

  Ces outils ont été conçus pour protéger l'identité des utilisateurs et chiffrer leurs communications. Ils peuvent aussi bien être utilisés par des acteurs légitimes (journalistes, militants des droits de l'homme, défenseurs de la vie privée) que par des cybercriminels.

**Le *Deep Web* comme le *Dark Web* font partie intégrante d'Internet, qui est un réseau de communication technologiquement neutre : n'importe quel contenu peut transiter à travers ce réseau.**

**Seuls les usages des internautes peuvent conduire à la commission d'infractions, en raison de la nature des contenus diffusés/consultés ou des produits ou services proposés/achetés.**

## 2. Le service Aleph SEARCH proposé par Aleph est-il licite ?

Oui, le service Aleph SEARCH est licite.

Il s'agit d'une technologie qui :

- procède à l'indexation de contenus explorés par les robots d'Aleph sur le *Deep Web* et du *Dark Web*,

- puis restitue les résultats d'indexation en fonction des requêtes et critères de recherche des utilisateurs.

A l'instar des moteurs de recherche grand public, les robots d'indexation d'Aleph SEARCH parcourent la toile du *Deep Web* et du *Dark Web* pour indexer et consulter l'ensemble des liens et pages qu'ils découvrent et qui sont accessibles sans porter atteinte à un système d'information.

Cette indexation est donc neutre technologiquement.

## 3. Le service Aleph ALERT proposé par Aleph est-il licite ?

Oui, le service Aleph ALERT est licite.

Il s'agit d'un tableau de bord permettant de visualiser les fuites de données correspondant à des mots-clés sélectionnés par ses clients.

Technologiquement parlant, il s'agit du même outil que le moteur de recherche Aleph SEARCH.

La différence est que les clients d'Aleph ne peuvent consulter que les résultats de mots-clés de recherche préalablement définis.

## 4. Quel est le statut juridique d'un moteur de recherche en ligne comme celui d'Aleph SEARCH ?

Les moteurs de recherche en ligne sont réglementés par le règlement européen 2022/2065 du 19 octobre 2022 « *Digital Services Act* » (ci-après le « **DSA** »).

L'article 3 j) du DSA définit le **moteur de recherche en ligne** comme :

> « ***un service intermédiaire*** *qui permet aux utilisateurs de formuler des requêtes afin d'effectuer des recherches sur, en principe, tous les sites internet ou tous les sites internet dans une langue donnée, sur la base d'une requête lancée sur n'importe quel sujet sous la forme d'un mot-clé, d'une demande vocale, d'une expression ou d'une autre entrée, et qui renvoie des résultats dans quelque format que ce soit dans lesquels il est possible de trouver des informations en rapport avec le contenu demandé* ».

L'article 3 g) du DSA définit les **services intermédiaires** comme :

> « *un des services de la société de l'information suivants : un service de « simple transport » (…) un service de « mise en cache » (…), un service d' « hébergement » (…)* ».

Le DSA n'indique pas précisément à quelle catégorie de services intermédiaires les moteurs de recherche en ligne doivent être assimilés.

Antérieurement au DSA, la jurisprudence européenne et française a assimilé les moteurs de recherche à des hébergeurs.

Tel a notamment été le cas du moteur de recherche en ligne de la société Google, dans de nombreuses décisions de justice.[1]

[1] CJUE, 23 mars 2010, aff. C-236/08, Google / Louis Vuitton Malletier | CJUE, 23 mars 2010, aff. C-237/08, Google / Viaticum SA et Luteciel SARL | CJUE, 23 mars 2010, aff. C-238/08, Google / CNRRH SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL | Cass. 1ère civ. 12 juillet 2012, n°11-15.165 et 11-15.188 | CA Paris, 9 avril 2014, n°13/05025 Google / Voyageurs du monde | CA Paris, 11 décembre 2013, n° 12/03071, Google / Olivier M. | CA Paris, 26 janvier 2011, n°08/13423 SAIF / Google | CA Paris, 19 novembre 2010, n°08/00620 Google / Syndicat français de la literie

## 5. Quelle est la responsabilité d'un moteur de recherche comme Aleph SEARCH en cas de référencement d'un contenu illicite ?

En premier lieu, les fournisseurs de moteur de recherche ne sont soumis à aucune obligation de surveillance ou de recherche active de contenus illicites.

En effet, l'article 8 du DSA dispose que :

> « *Les fournisseurs de services intermédiaires* [dont les moteurs de recherche en ligne] *ne sont soumis à* ***aucune obligation générale de surveiller*** *les informations qu'ils transmettent ou stockent o****u de rechercher activement des faits ou des circonstances révélant des activités illégales.*** »

En second lieu, les fournisseurs de moteur de recherche bénéficient du régime de responsabilité atténué reconnu aux hébergeurs.

Le considérant 28 du DSA dispose que les fournisseurs de moteurs de recherche en ligne bénéficient de ce régime de responsabilité atténué :

> *« (…) À cet égard, il convient de rappeler que* ***les fournisseurs de services établissant et facilitant l'architecture logique sous-jacente et le bon fonctionnement de l'internet****, y compris les fonctions techniques accessoires,* ***peuvent également bénéficier des exemptions de responsabilité prévues par le présent règlement****, dans la mesure où leurs services peuvent être qualifiés de services de "simple transport", de "mise en cache" ou d'"hébergement". **De tels services comprennent, (…) les moteurs de recherche en ligne**, (…). **Ces services peuvent également bénéficier d'exemptions de responsabilité, dans la mesure où ils peuvent être qualifiés de services** de "simple transport", de "mise en cache" ou **d'"hébergement".** »*

Le régime de responsabilité atténué applicable aux hébergeurs est le suivant (Article 16 1 du DSA) :

> *« 1. En cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service,* ***le fournisseur de services n'est pas responsable*** *des informations stockées à la demande d'un destinataire du service* ***à condition que le fournisseur :***
>
> *a)* ***n'ait pas effectivement connaissance de l'activité illégale ou du contenu illicite*** *et, en ce qui concerne une demande en dommages et intérêts, n'ait pas conscience de faits ou de circonstances selon lesquels l'activité illégale ou le contenu illicite est apparent;*
>
> ***ou***
>
> *b)* ***dès le moment où il en prend connaissance ou conscience, agisse promptement pour retirer le contenu illicite ou rendre l'accès à celui-ci impossible****. »*

La connaissance d'un contenu illicite doit être spécifique et ne peut pas être acquise de façon générale.

En effet, le considérant 22 du DSA dispose :

> *« (…)* ***cette connaissance*** *ou prise de conscience effective* ***ne peut être considérée comme étant présente au seul motif que le fournisseur est conscient, de manière générale, que son service est également utilisé pour stocker des contenus illicites****. »*

**Ainsi, l'éditeur d'un moteur de recherche en ligne n'est pas responsable des contenus illicites qu'il référence ; il ne le devient que si, ayant eu connaissance au cas par cas de leur illicéité, il ne les a pas retiré promptement.**

## 6. Pourquoi Aleph ne recherche pas de façon offensive les fuites de données comme d'autres prestataires ?

Aleph se limite à indexer et référencer des sites internet, c'est-à-dire des informations volontairement rendues publiques. Ce fonctionnement licite est celui d'un moteur de recherche (voir ci-avant 2).

En revanche, Aleph ne procède pas à la recherche offensive d'informations pouvant être accessibles en raison d'un défaut de sécurité ou de l'exploitation d'une vulnérabilité d'une machine (serveur, ordinateur, etc.).

En effet, il n'existe aucun motif légitime à rechercher activement des fuites de données en scannant des machines connectées à Internet, en y accédant puis en y extrayant des données.

**Au contraire, ces pratiques d'autres prestataires sont répréhensibles pénalement puisqu'elles constituent le délit :**

- **d'accès et de maintien frauduleux** dans un système de traitement automatisé de données (STAD), puni de 5 ans d'emprisonnement et de 100 000 € d'amende (323-1 du Code pénal),

- **et d'extraction frauduleuse de données** d'un STAD, puni de 5 ans d'emprisonnement et de 150 000 € d'amende (323-3 du Code pénal).

Lorsqu'elles sont commises par des personnes morales, le montant maximal de ces amendes est égal au quintuple des montants ci-avant indiqués, conformément à l'article 131-38 du Code pénal.

En outre, **la simple tentative** d'accéder, de se maintenir ou d'extraire des données d'un STAD **est punie des mêmes peines** (323-7 du Code pénal).

**Ces pratiques illicites engagent également la responsabilité pénale des clients qui recourent à de tels prestataires, puisqu'ils peuvent à leur tour être poursuivis pénalement du délit :**

- **de détention ou d'utilisation de données provenant frauduleusement d'un STAD**, puni de 5 ans d'emprisonnement et de 150 000 € d'amende (323-3 du Code pénal).

- **et de complicité** conformément à l'article 121-6 du Code pénal.

## 7. La recherche sur internet de fuite d'informations (RIFI) est-elle licite ?

**Oui, sous certaines conditions : la seule légitimité d'un client à réaliser une RIFI n'est pas suffisante pour la rendre licite.**

La licéité de la RIFI va notamment dépendre de sa finalité et des modalités de sa mise en œuvre.

En premier lieu, la finalité doit viser à rechercher des fuites de données concernant le client.

> *Exemple : le client doit utiliser des mots clefs liés à des informations le concernant.*

Elle ne doit pas être destinée à rechercher ni accéder à des fuites de données affectant des tiers (ex. : des concurrents) et révélant des données à caractère personnel, des informations confidentielles ou stratégiques.

En deuxième lieu, les modalités de mise en œuvre de la RIFI doivent respecter la réglementation.

Aucune atteinte à un STAD ne doit être réalisée pour accéder aux données (voir ci-avant 6).

> *Exemple : le client ou son prestataire ne doivent pas exploiter de vulnérabilités ou contourner des mécanismes de sécurité pour accéder à des informations.*

Seules les informations accessibles sans contournement de sécurité doivent être analysées.

En troisième lieu, lorsque l'analyse révèle des informations ne concernant pas le client, celles-ci ne doivent ni être extraites ni conservées.

> *Exemple : Malgré des mots clefs pertinents, les résultats de la RIFI peuvent renvoyer des faux positifs ou des informations ne concernant pas le client.*

Dès que le client acquiert la conviction que les données auxquelles il accède ne le concerne pas, il ne devrait pas poursuivre leur consultation ni en prendre copie.

En quatrième lieu, la RIFI nécessite de se conformer au RGPD, et notamment les recommandations de la CNIL[2].

> *Exemple : Le client ne pourra dupliquer que les preuves de fuites de données provenant de son SI et devra minimiser la collecte de données personnelles.*

La licéité d'une RIFI suppose ainsi une réflexion en amont de son périmètre (finalité, mots clés) et de ses modalités de réalisation.

[2] https://www.cnil.fr/fr/la-recherche-sur-internet-de-fuites-dinformations-rifi

## 8. Pourquoi la RIFI nécessite la signature d'un mandat ?

La signature d'un mandat n'est exigée que lorsque Aleph intervient humainement dans la réalisation d'une RIFI.

Dans ce cadre, le mandat formalise l'autorisation donnée par le client d'agir en son nom et pour son propre compte afin de rechercher des fuites d'informations provenant de son patrimoine informationnel.

Ce mandat matérialise l'autorisation expresse et spécifique du client et protège Aleph de toute mise en cause de sa responsabilité au titre d'une éventuelle atteinte au système de traitement automatisé de données du client et des données qu'il contient.

Ce mandat est uniquement nécessaire lorsqu'un client demande à Aleph de réaliser une RIFI. En revanche, le mandat n'est pas nécessaire lorsqu'un client utilise les services d'Aleph en toute autonomie.

* * *