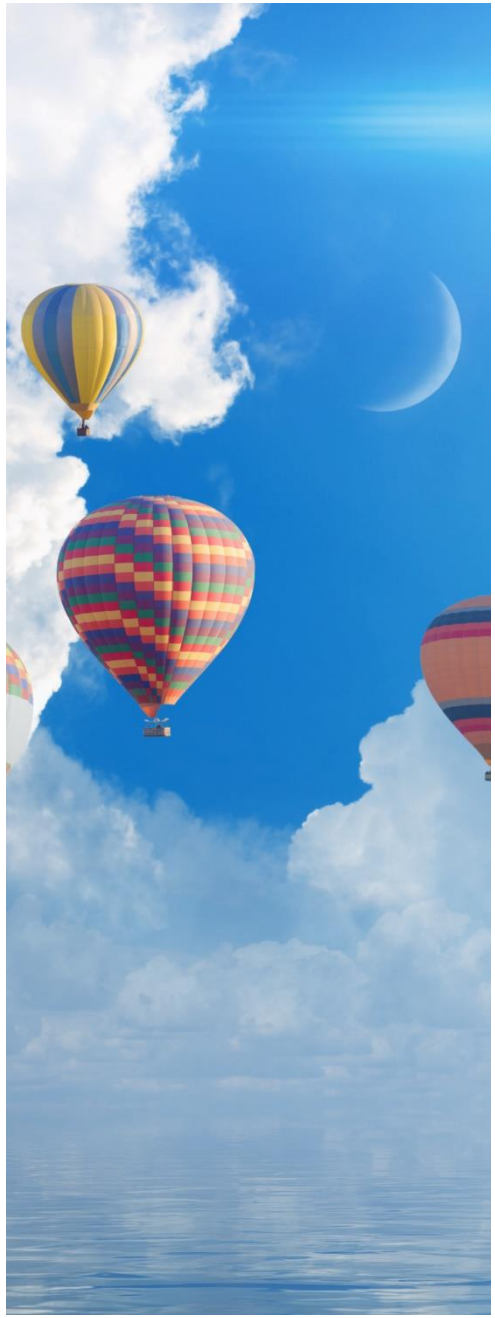
racine
AVOCATS

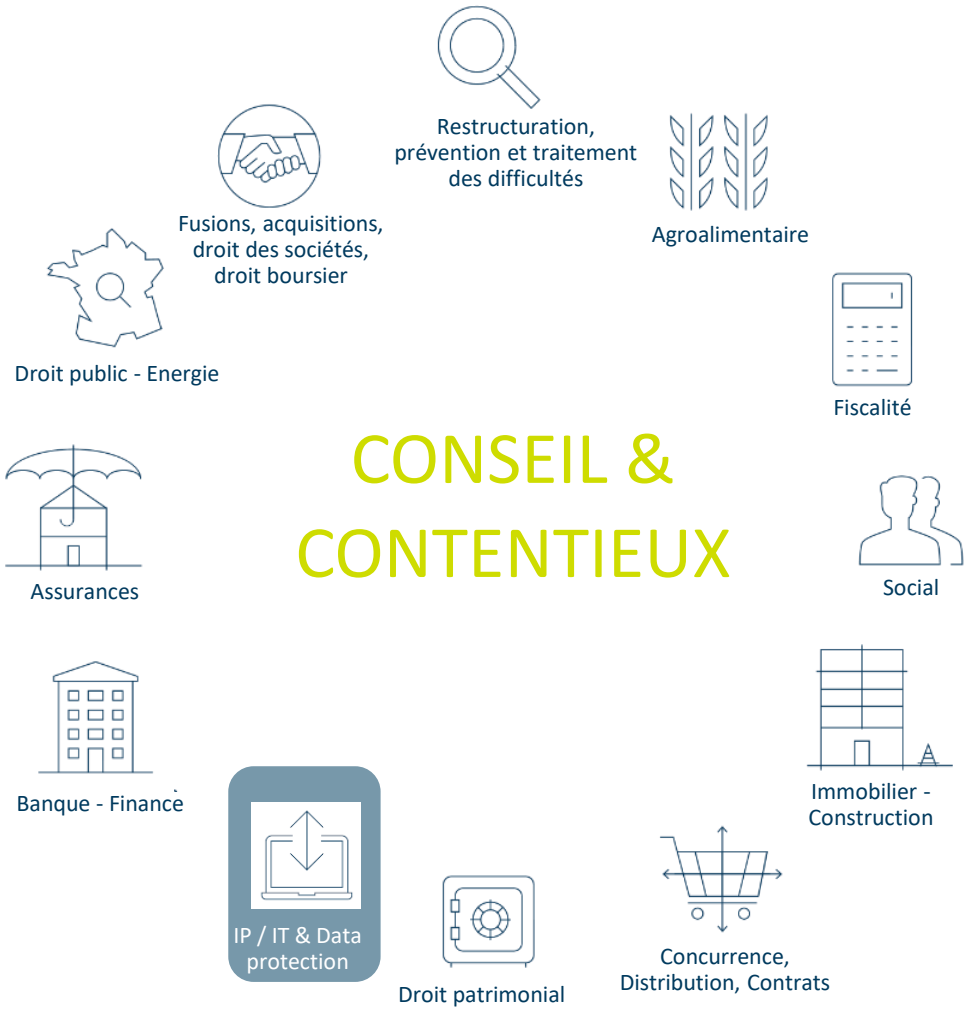
Veille et investigation en ligne



Quels risques légaux pour la veille et l'investigation en ligne ?

Groupe "Club OSINT & Veille"

Racine vous connaissez …



Mais connaissez vous l’équipe IP – IT & Data Protection

Eric Barbry
Associé
ebarbry@racine.eu

Eric accompagne les entreprises dans le cadre de leur transformation digitale. Il accompagne également les pur player du secteur du numérique. Il possède dans les trois domaines de l’IP, IT et de la protection des données.

Dans le domaine de l’IP Property) l’équipe intervient dans tous les domaines relatifs à la valorisation du patrimoine immatériel des entreprises et acteurs publics (marques, noms de domaine, brevets, concepts algorithmes, …).

En matière IT l’équipe dispose d’une compétence tout à fait particulière Elle intervient en conseil, contentieux et contrats dans les domaines suivant : internet, plateformes et commerce électronique, marketing digital, télécommunications, applications mobiles, dématérialisation ou encore sécurité des systèmes d’information.

En matière de Data, l’équipe intervient quotidiennement dans le domaine du droit des données à caractère personnel et le déploiement du RGPD. Mais elle intervient également sur le droit des data de manière plus générales (open data, données d’intérêt public, confidentiel entreprises, secret, …).

Domaines d’expertise

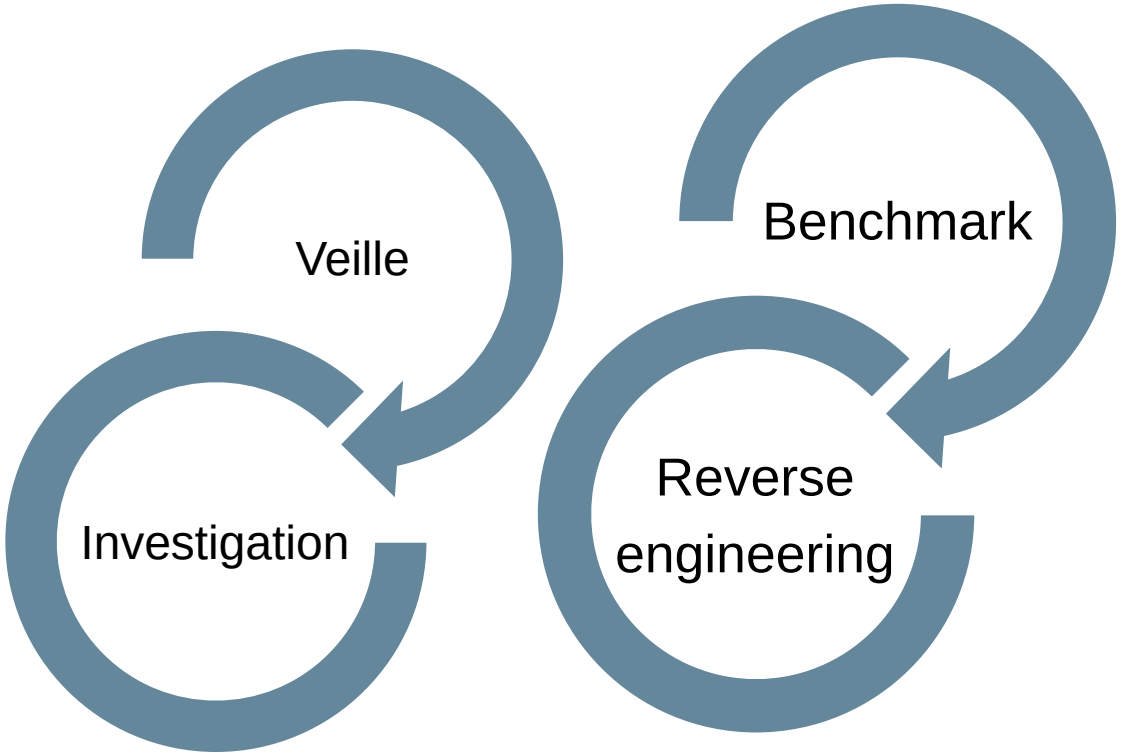
- Intellectual property
- Information technology
- Data Protection
- Sécurité des SI
- Droit de dématérialisation

racine
AVOCATS

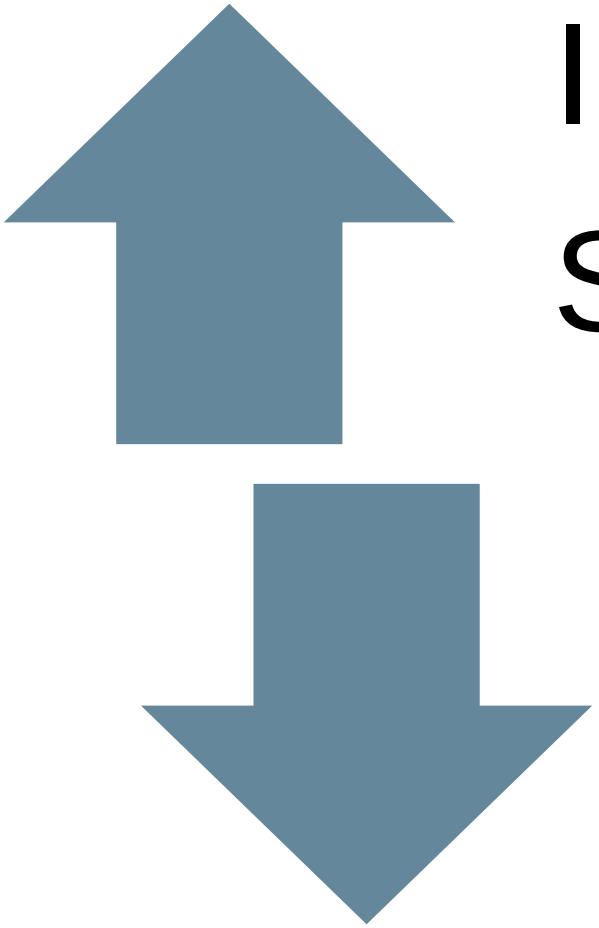
PARTIE 1

Veille et investigation – Un droit, voir une obligation…

Ceci n’est pas interdit …



Certaines investigations sont nécessaires



Interne

Sapin 2

Externe

KYC

racine
AVOCATS

PARTIE 2

Dura lex send lex

Ceci est interdit …

Article 323-1 Code pénal

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende. »

Article 323-3 Code pénal

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende. »

Le cas particulier des données personnelles

Art. 226-18 code pénal

Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Dommages collatéraux

Article 323-2 Code pénal

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende ».

Article 323-3-1 Code pénal

« Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

Article 323-6 Code pénal

« Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise. »

Le droit des bases de données

Article L.342-1 du code de la propriété intellectuelle

« Le producteur de bases de données a le droit d'interdire :

1° L'extraction, par transfert permanent et temporaire de la totalité ou d'une partie qualitativement et quantitativement substantielle du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit ;

2° La réutilisation, par la mise à la disposition du public de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, quelle qu'en soit la forme ».

Article L.342-2 du CPI

« Le producteur peut également interdire l'extraction ou la réutilisation répétée et systématique de parties qualitativement ou quantitativement non substantielles du contenu de la base lorsque ces opérations excèdent manifestement les conditions d'utilisation normale de la base de données ».

Le secret des affaires….

Article L151-1 (code de commerce - LOI n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires - 30 juillet 2018)

« Est protégée au titre du secret des affaires toute information répondant aux critères suivants :

1° Elle n'est pas, en elle-même ou dans la configuration et l'assemblage exacts de ses éléments, généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité ;

2° Elle revêt une valeur commerciale, effective ou potentielle, du fait de son caractère secret ;

3° Elle fait l'objet de la part de son détenteur légitime de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret. »

Article L151-2 (Code commerce)

« Est détenteur légitime d'un secret des affaires celui qui en a le contrôle de façon licite ».

Le caractère illicite

Article L151-4

« L'obtention d'un secret des affaires est illicite lorsqu'elle est réalisée sans le consentement de son détenteur légitime et qu'elle résulte :

1° D'un accès non autorisé à tout document, objet, matériau, substance ou fichier numérique qui contient le secret ou dont il peut être déduit, ou bien d'une appropriation ou d'une copie non autorisée de ces éléments ;

2° De tout autre comportement considéré, compte tenu des circonstances, comme déloyal et contraire aux usages en matière commerciale. »

Article L151-5

« L'utilisation ou la divulgation d'un secret des affaires est illicite lorsqu'elle est réalisée sans le consentement de son détenteur légitime par une personne qui a obtenu le secret dans les conditions mentionnées à l'article L. 151-4 ou qui agit en violation d'une obligation de ne pas divulguer le secret ou de limiter son utilisation.

La production, l'offre ou la mise sur le marché, de même que l'importation, l'exportation ou le stockage à ces fins de tout produit résultant de manière significative d'une atteinte au secret des affaires sont également considérés comme une utilisation illicite lorsque la personne qui exerce ces activités savait, ou aurait dû savoir au regard des circonstances, que ce secret était utilisé de façon illicite au sens du premier alinéa du présent article. »

Article L151-6

« L'obtention, l'utilisation ou la divulgation d'un secret des affaires est aussi considérée comme illicite lorsque, au moment de l'obtention, de l'utilisation ou de la divulgation du secret, une personne savait, ou aurait dû savoir au regard des circonstances, que ce secret avait été obtenu, directement ou indirectement, d'une autre personne qui l'utilisait ou le divulguait de façon illicite au sens du premier alinéa de l'article L. 151-5. »

racine
AVOCATS

PARTIE 3

Mais alors on ne peut rien faire !

Sur quoi porte la veille ou les investigations

Veille et investigation « en ligne »

- Internet
- Plateforme et extranet
- Mobile

Mais alors on peut rien faire ?

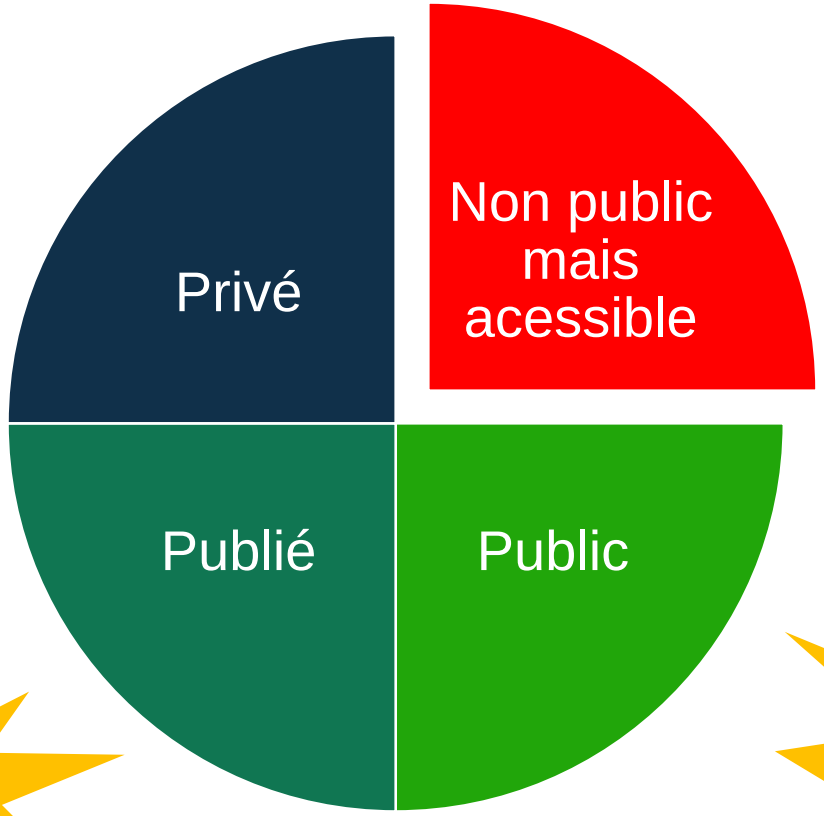
Article L151-3 du code de commerce

« Constituent des modes d'obtention licite d'un secret des affaires :

1° Une découverte ou une création indépendante ;

2° L'observation, l'étude, le démontage ou le test d'un produit ou d'un objet qui a été mis à la disposition du public ou qui est de façon licite en possession de la personne qui obtient l'information, sauf stipulation contractuelle interdisant ou limitant l'obtention du secret. »

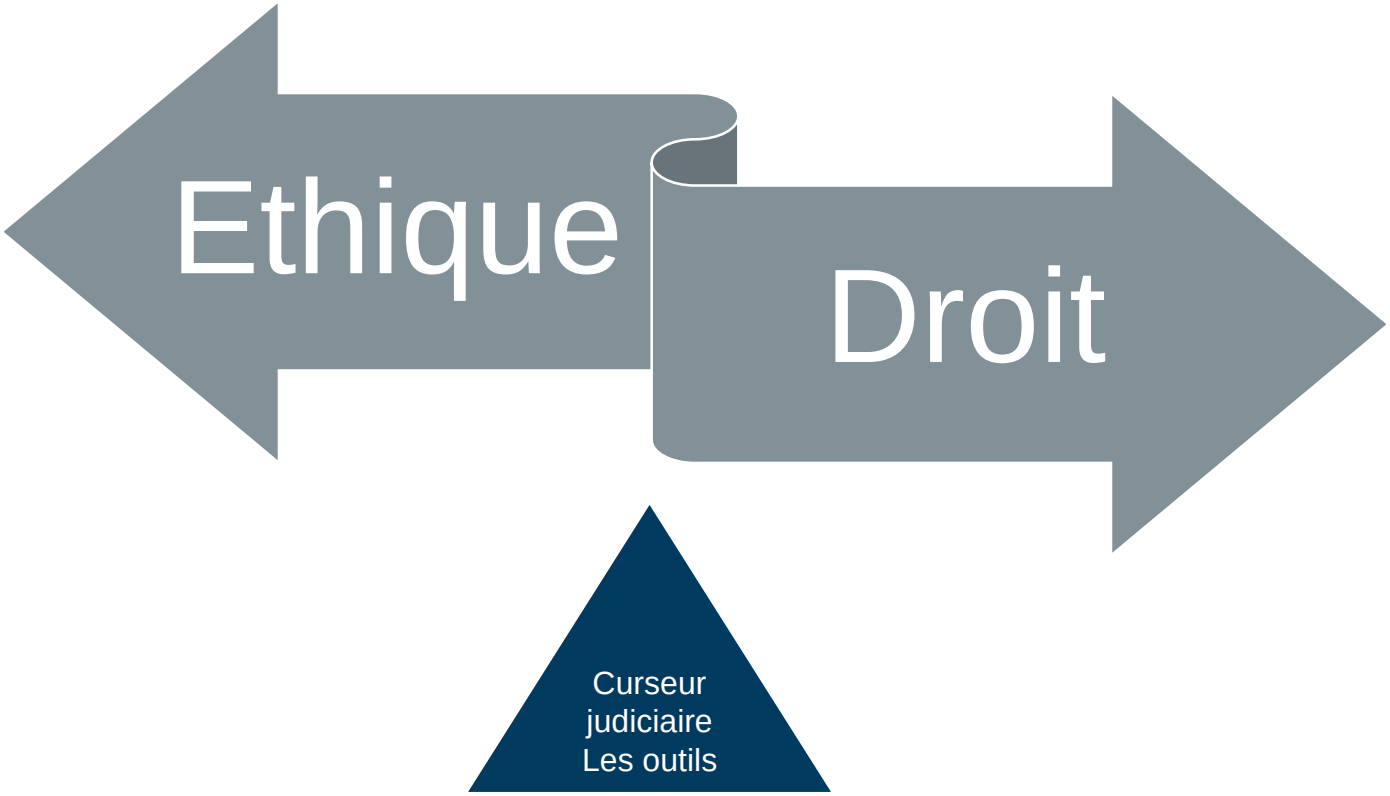
La vraie question



Concurrence déloyale

Propriété intellectuelle – confidentiel entreprise

La seule question



racine
AVOCATS

PARTIE 4

La jurisprudence

Jurisprudence française

Démarche d'acquisition - Le cas … weezevent

Investigation de protection – Le cas Petit Bateau

Weezevent et scrapping

* Sur l'accès et le maintien frauduleux dans un système de traitement automatisé de données :

C'est à bon escient que les premiers juges ont relaxé l'appelant de l'infraction d'accès frauduleux de données dans un système de traitement automatisé de données, en raison d'une part de l'accès ouvert au public du site Weezevent et d'autre part, de l'absence de mise en place d'une protection du site ou de la manifestation de la volonté du dirigeant du site de restreindre l'accès au système informatisé de données. Il n'y a pas eu utilisation d'un mode irrégulier de pénétration dans le système de traitement automatisé de données de Weezevent.

M. X. s'est maintenu sur le site qui n'avait aucune protection particulière. Les données étaient accessibles au public. Il n'est pas davantage établi qu'il se soit maintenu frauduleusement sur le site de Weezevent.

L'intention frauduleuse résulte de l'utilisation de scripts spécialement conçus par M. X. pour effectuer automatiquement une collecte sélective de données qui a en outre été réalisée dans un but concurrentiel, tel que cela ressort clairement des mails échangés par le prévenu avec des proches.

Les données copiées et tirées du site Weezevent étaient certes accessibles au public mais par la façon automatisée et sélective de procéder, cela a entraîné l'extraction importante de 44 380 fichiers dont 7 779 étaient retrouvés sur le site de M. X. soit environ 16% des données du site victime sachant que ces données ne pouvaient être extraites sans autorisation expresse de Weezevent. Or, M. X. a agi à l'insu du directeur du site Weezevent par des moyens techniques conçus à cet effet par l'appelant. L'infraction est établie et applicable pour les faits reprochés à M. X. à compter de la loi soit du 13 novembre 2014 jusqu'au 15 mars 2015. M. X. doit être relaxé pour les faits visés dans la prévention du 3 juillet 2014 au 12 novembre 2014.

Compte facebook – Petit Bateau

Réponse de la Cour

5. D'abord, si en vertu du principe de loyauté dans l'administration de la preuve, l'employeur ne peut avoir recours à un stratagème pour recueillir une preuve, la cour d'appel, qui a constaté que la publication litigieuse avait été spontanément communiquée à l'employeur par un courriel d'une autre salariée de l'entreprise autorisée à accéder comme « amie » sur le compte privé Facebook de Mme X..., a pu en déduire que ce procédé d'obtention de preuve n'était pas déloyal.

6. Ensuite, il résulte des articles 6 et 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 9 du code civil et 9 du code de procédure civile, que le droit à la preuve peut justifier la production d'éléments portant atteinte à la vie privée à la condition que cette production soit indispensable à l'exercice de ce droit et que l'atteinte soit proportionnée au but poursuivi.

7. La production en justice par l'employeur d'une photographie extraite du compte privé Facebook de la salariée, auquel il n'était pas autorisé à accéder, et d'éléments d'identification des « amis » professionnels de la mode destinataires de cette publication, constituait une atteinte à la vie privée de la salariée.

8. Cependant, la cour d'appel a constaté que, pour établir un grief de divulgation par la salariée d'une information confidentielle de l'entreprise auprès de professionnels susceptibles de travailler pour des entreprises concurrentes, l'employeur s'était borné à produire la photographie de la future collection de la société publiée par l'intéressée sur son compte Facebook et le profil professionnel de certains de ses « amis » travaillant dans le même secteur d'activité et qu'il n'avait fait procéder à un constat d'huissier que pour contrecarrer la contestation de la salariée quant à l'identité du titulaire du compte.

9. En l'état de ces constatations, la cour d'appel a fait ressortir que cette production d'éléments portant atteinte à la vie privée de la salariée était indispensable à l'exercice du droit à la preuve et proportionnée au but poursuivi, soit la défense de l'intérêt légitime de l'employeur à la confidentialité de ses affaires.

Jurisprudence étrangère

L’affaire LinkedIn c/ HiQ

Une vision diamétralement opposée

Pour toutes ces raisons, il apparaît que l'interdiction de la CFAA d'accéder à un ordinateur "sans autorisation" est violée lorsqu'une personne contourne les règles généralement applicables en matière d'autorisations d'accès à un ordinateur, telles que les exigences relatives au nom d'utilisateur et au mot de passe, pour accéder à un ordinateur. Il est probable que lorsqu'un réseau informatique permet généralement l'accès public à ses données, l'accès d'un utilisateur à ces données accessibles au public ne constituera pas un accès sans autorisation en vertu de la CFAA. Les données auxquelles l'utilisateur cherche à accéder ne sont pas la propriété de LinkedIn et n'ont pas été délimitées par LinkedIn comme étant privées en utilisant un tel système d'autorisation. HiQ a donc soulevé de sérieuses questions quant à savoir si LinkedIn peut invoquer la CFAA pour devancer la réclamation d'interférence délictuelle éventuellement méritoire de HiQ.[12]

- Fraude informatique = non

Pour sa part, LinkedIn fait valoir que l'injonction préliminaire est contraire à l'intérêt public car elle invitera des acteurs malveillants à accéder aux ordinateurs de LinkedIn et à attaquer ses serveurs. En conséquence, selon l'argument, LinkedIn et d'autres sociétés ayant des sites web publics seront obligées de choisir entre laisser leurs serveurs ouverts à de telles attaques ou protéger leurs sites web par des mots de passe, les coupant ainsi de la vue du public.

Bien qu'il y ait des intérêts publics importants des deux côtés, le tribunal de district a correctement déterminé que, tout compte fait, l'intérêt public favorise la position de HQ. Nous sommes d'accord avec le tribunal de district pour dire que donner carte blanche à des sociétés comme LinkedIn pour décider, sur n'importe quelle base, qui peut collecter et utiliser des données - des données qui ne sont pas la propriété des sociétés, qu'elles rendent autrement accessibles au public et que les sociétés elles-mêmes collectent et utilisent - risque de créer des monopoles de l'information qui ne serviraient pas l'intérêt public.

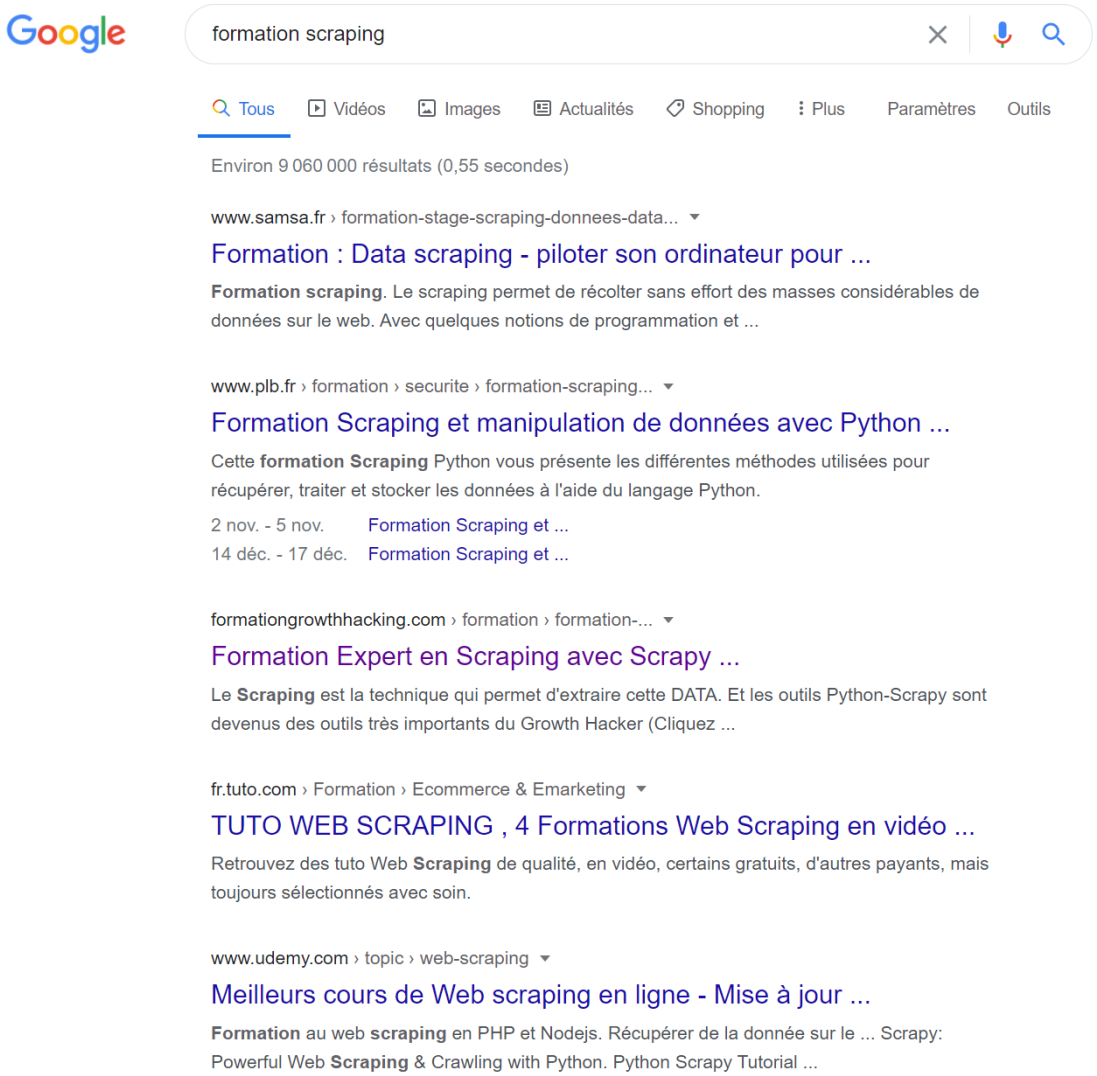
- Intérêt public = non

racine
AVOCATS

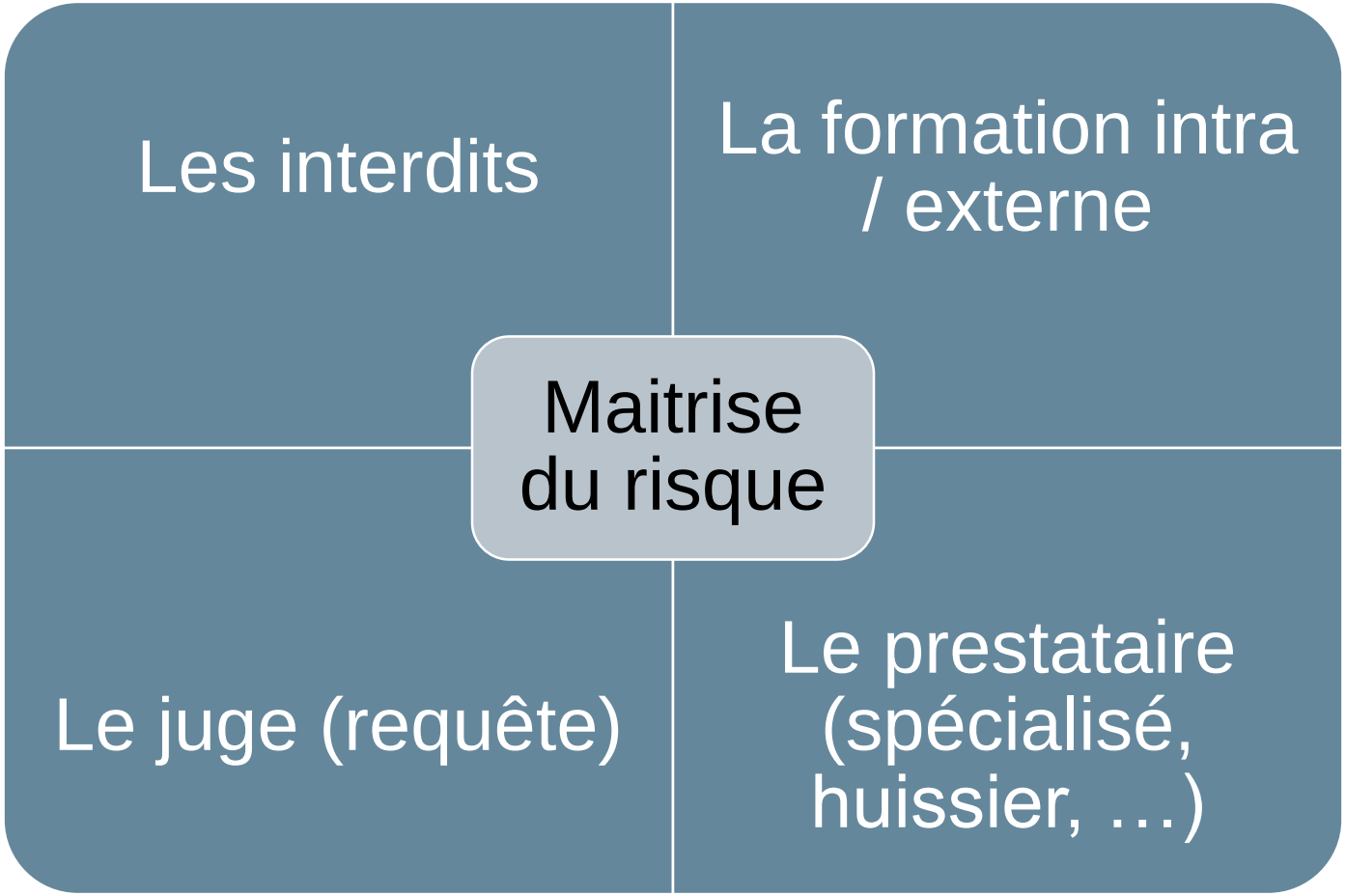
PARTIE 5

Une veille ou investigation maîtrisée

Trouver une formation… facile

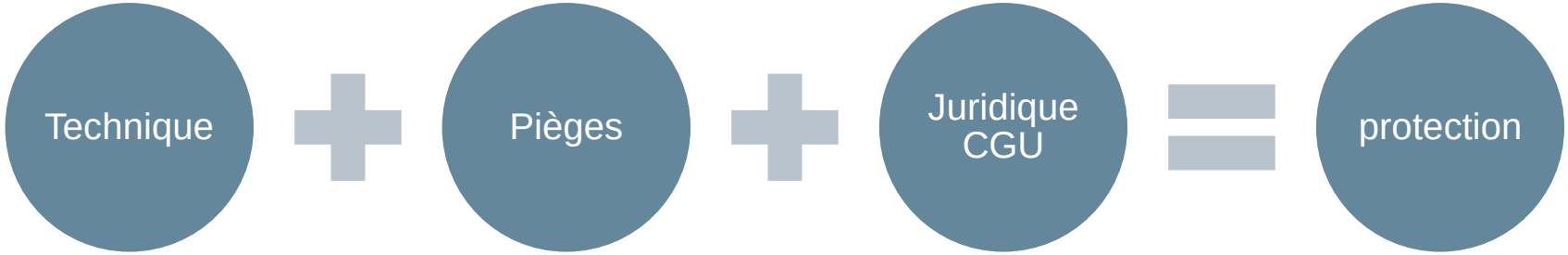


En « demande »


Les interdits
La formation intra / externe
Maitrise du risque
Le juge (requête)
Le prestataire (spécialisé, huissier, …)

Une analyse au cas par cas est nécessaire

En « défense »



Merci pour votre attention

C’est le temps des échanges