n°91
[août- septembre - octobre]

LE JOURNAL DU VILLAGE DE LA JUSTICE

www.village-justice.com

legi team Editions

Revue du Web juridique - p49

Annonces d'emploi - p50

abcliv.fr

Depuis 1978

Spécialiste et conseil
EN DOMICILIATION D'ENTREPRISE

À VOTRE SERVICE AVEC SES 42 ANS D'EXPERIENCE

RCS 314 503 996

L'adresse de votre siège social et fiscal à partir de **18€**

AVANT DE VOUS ENGAGER, CALCULEZ LE COÛT DE VOTRE DOMICILIATION EN 3 CLICS !
www.abcliv.fr

EFFECTUEZ LES FORMALITÉS DE VOS CLIENTS DANS LES MEILLEURS DÉLAIS PAR SIMPLE APPEL TÉLÉPHONIQUE À L'UNE DE NOS COLLABORATRICES QUI VOUS FERA PARVENIR L'ENGAGEMENT DE DOMICILIATION PAR RETOUR.

GRATUITÉ DU DÉPÔT DE DOSSIERS AUPRÈS DU GREFFE DE PARIS
(si domiciliation en nos bureaux)

RÉTROCESSION D'HONORAIRES POUR TOUT NOUVEAU CONTRAT DE DOMICILIATION

Cette rétrocession correspond à 50% sur le montant ht de la 1er facture d'inscription. Le règlement vous sera adressé suite à la réception de la facture rappelant les références du client domicilié, à envoyer chez ABC LIV 38 rue Servan 75544 Paris cedex 11 (non cumulable avec tout autre promotion)

33 ADRESSES EN ILE DE FRANCE

Accueil et informations sans rendez-vous dans toutes nos agences du Lundi au Vendredi

01er	23/25 rue J. J. Rousseau	26 €
02è	12 rue Vivienne	30 €
03è	21 place de la République	32 €
04è	14 rue Charles V	22 €
05è	16 bd St Germain	28 €
06è	99/103 rue de Sèvres	24 €
07è	31 avenue de Ségur	18 €
08è	37 rue des Mathurins	36 €
08è	91 rue du Fbg Saint Honoré	36 €
08è	66 av des Champs Elysées	36 €
08è	49 rue de Ponthieu	36 €
08è	128 rue La Boëtie	36 €
09è	42 rue de Maubeuge	22 €
10è	32 bd de Strasbourg	20 €
11è	38 rue Servan	26 €
12è	9 rue Parrot	24 €
13è	38 rue Dunois	20 €
14è	23 rue du Départ	26 €
14è	16 bis rue d'Odessa	26 €
14è	101 av. du Général Leclerc	18 €
14è	48 rue de Sarrette	18 €
15è	366 ter rue de Vaugirard	26 €
16è	111 avenue Victor Hugo	34 €
17è	23 rue Nollet	28 €
18è	21 bis rue du Simplon	22 €
18è	26 rue Damremont	22 €
19è	118/130 avenue Jean Jaurés	22 €
19è	103 bd Mac Donald	22 €
20è	2 bis rue Dupont de l'Eure	22 €
92100	47 rue M. Dassault (Boulogne)	36 €
92200	176 av. Ch de Gaulle (Neuilly/Seine)	38 €
93100	95 av. du Pr. Wilson (Montreuil)	28 €
94300	112 av. de Paris (Vincennes)	28 €

Tarifs 2020 mensuels HT pour les nouveaux clients non cumulable sur présentation du journal en cours, lors de l'inscription.

LE JOURNAL DU VILLAGE DE LA JUSTICE

est édité par LEGI TEAM
198 avenue de Verdun
92130 Issy-les-Moulineaux
Tél. : 01 70 71 53 80
Fax : 01 46 09 13 85
www.legiteam.fr

DIRECTEUR DE LA PUBLICATION
Emmanuel FONTES

RÉDACTRICE EN CHEF
Aude Dorange

ABONNEMENTS
Emmanuel FONTES
Tél. : 01 70 71 53 89

MAQUETTE
Cyriane VICIANA
pao@legiteam.fr

Dépôt Légal N ° 99027
ISSN : 2257-4581

PUBLICITÉ
Régie exclusive : LEGI TEAM
Emmanuel FONTES
e.fontes@legiteam.fr
Tél. : 01 70 71 53 89

IMPRIMEUR
ROTIMPRESS
POL. IND. CASA NOVA - CARRER PLA DE L'ESTANY S/N
17181 AIGUAVIVA (GIRONA)

DIFFUSION AVOCATS
16 000 exemplaires

ÉDITO

La cyber sécurité des cabinets d'avocats

Les cyberattaques sont un véritable fléau à l'échelle mondiale et on ne compte plus le nombre d'entreprises victimes de failles de sécurité relatives aux informations sur leur clientèle : noms, adresses, numéros de téléphone ou encore données bancaires qui sont détruites, altérées, divulguées publiquement…

Les raisons sont multiples. Certes, il peut y avoir des motifs de vengeance à l'initiative d'anciens salariés, partenaires ou prestataires… mais il s'agit le plus souvent d'actes de négligences ou d'imprudence : un dispositif de protection trop léger, l'utilisation sans encadrement des objets connectés en lien avec les serveurs, le recours à des wifi publics non sécurisés, un manque de formation des collaborateurs aux règles essentielles de « l'hygiène informatique »... Quiconque disposant d'un ordinateur et de quelques connaissances pratiques peut infiltrer un écosystème mal protégé.

Or, en présence d'une faille de sécurité, le responsable du traitement se retrouve en première ligne. Il doit notifier à l'autorité de contrôle et aux personnes concernées la violation de données. Le défaut de sécurisation expose à de lourdes sanctions pénales et administratives. Il faut également compter avec les conséquences souvent désastreuses en termes d'image. Il est donc urgent de prendre conscience des risques liés à la cybersécurité.

Cette préoccupation prend un relief particulier avec le déploiement massif du télétravail à l'heure du Covid-19. En effet, 29% seulement des personnes interrogées dans le cadre d'un récent sondage indiquent prévoir une protection spécifique sur les PC des collaborateurs à domicile alors que les attaques sur les appareils personnels et les appareils mobiles des collaborateurs s'amplifient ! En d'autres termes, la pandémie de Covid-19 a provoqué celle de la cybercriminalité.

Tous les secteurs sont concernés. Les cabinets d'avocat n'y échappent donc pas, à l'exemple du cabinet new-yorkais Grubman Shire Meiselas & Sacks, victime d'une attaque de *ransomware*[1]. Ayant refusé de payer la rançon de 42 millions de dollars exigée par les hackers, des données confidentielles de clients médiatiques ont été rendues publiques, à l'instar de celles concernant Lady Gaga, occasionnant un très lourd préjudice économique et réputationnel au cabinet.

1 - Le *ransomware* est un logiciel malveillant prenant en otage les données présentes sur votre ordinateur en les chiffrant. Une fois les données rendues inaccessibles pour l'utilisateur, le pirate exige le paiement d'une rançon en contrepartie de la livraison de la clé de déchiffrement.

ÉDITO

Les avocats sont donc directement responsables de la sécurité des données à caractère personnel de leurs clients, mais aussi de leurs données stratégiques, et il leur appartient d'anticiper et de circonscrire le risque des attaques qui peuvent survenir à tout moment.

Comme dans toute entreprise, ils doivent appliquer, au sein de leur cabinet, certaines règles : gérer strictement les accès aux serveurs et attribuer des niveaux d'habilitation en fonction des besoins réels des utilisateurs, supprimer les comptes des anciens collaborateurs, faire les mises à jour des logiciels de sécurité (même si cela oblige à redémarrer l'ordinateur !), disposer d'une politique de mots de passe robuste (imposer un nombre et une typologie de caractères, imposer une modification régulière des mots de passe, refuser leur communication à toute autre personne que son titulaire, etc.) … autant de précautions basiques qui sont encore trop peu souvent mises en application.

De même, prendre des renseignements sur le prestataire informatique pressenti, sur les normes de sécurité qu'il propose, lui faire signer un engagement de confidentialité, encadrer les conditions d'intervention des services d'assistance (conditions d'accès à distance ou accès aux locaux), interdire toute sous-traitance sans accord préalable… sont autant de précautions indispensables pour prévenir les risques d'intrusion ou d'altération des données dont nous avons la responsabilité.

Il peut être utile de désigner un Délégué à la protection des données (DPD souvent désigné DPO : Data Protection Officer) pour veiller au respect des mesures de sécurité en conformité avec le RGPD. Celui-ci peut également avoir pour mission de sensibiliser et de former les collaborateurs et le personnel administratif. Le réflexe « sécurité » s'apprend et exige un suivi constant.

Il existe de nombreux guides pour instaurer les bonnes pratiques et les mesures de précaution standard. Ceux de l'ANSSI[2] ou encore de la CNIL[3]… et bien sûr celui du CNB, spécifique à la profession, mis en ligne depuis 2018[4] qui précise les obligations à la charge des cabinets d'avocat. Il existe également des formations sur le sujet : les MOOC de l'ANSSI et de la CNIL évidemment, mais aussi les e-learning conçus par le Conseil National des Barreaux et proposés par les écoles d'avocats sur la protection des données personnelles, la cybersécurité et la cybercriminalité dont les prochaines sessions démarrent mi-septembre.

Les mesures à mettre en place sont certes contraignantes, mais elles sont indispensables pour préserver la confidentialité et le secret professionnel. Inutile en effet de se battre pour préserver le secret professionnel si on utilise des adresses e-mail non sécurisées et si les données de nos clients peuvent être appréhendées par des tiers !

C'est dire que désormais la cybersécurité fait partie de la pratique quotidienne de l'avocat et qu'il est indispensable de s'y former.

Christiane Féral-Schuhl, Présidente du Conseil National des Barreaux.

2 - ANSSI, Guide de l'hygiène informatique, renforcer la sécurité de son système d'information en 42 mesures, janvier 2017.

3 - CNIL, les guides de la CNIL, La sécurité des données personnelles, 2018

4 - CNB, guide, Les avocats et le règlement général sur la protection des données, mars 2018, Fiches pratiques n°2 et 8.

Comment nos logiciels de gestion Kleos et LOP répondent à la sécurité des données des cabinets d'avocats ?

1. PROTECTION DES TRANSMISSIONS

- **Le site hébergeant nos logiciels est sécurisé et certifié**
- **Protection contre les virus, les logiciels malveillants et le phishing** par des services reconnus dans la protection tels que McAfee et Norton, qui examinent aussi les autres risques de vulnérabilité.
- **Connection https sécurisée et certifiée lors de vos transferts de données.** La transmission de données, faite via le protocole HTTPS, est cryptée avec le certificat 2048-bit PKI et **certifié par Norton.**

2. PROTECTION & DISPONIBILITÉ DES DONNÉES

- **Serveurs hébergés en France et en Allemagne** et certifiés aux normes sécurité des données les plus élevées: **ISO 27 001, SAS-70 Type II.**
- **Centre d'hébergement de niveau Tier IV en conformité avec les règles européennes concernant le caractère privé des données.**
- **Disponibilité du serveur de 99,995% et accès continu à l'applicatif Kleos**, continuité de service et système supervisé 24/7.
- **Sauvegarde des données :** sauvegarde complète des données clients tous les soirs pour assurer la protection des données contre des actes malveillants ou des erreurs.
- Une équipe de **15 ingénieurs veille quotidiennement à la sécurité et à la disponibilité des serveurs.**

3. CONTRÔLES DES ACCÈS AUX DONNÉES

- Les bâtiments et serveurs sont protégés des intrusions et attaques.
- Aucun accès aux données pour les personnes non-autorisées.
- **Les données sont hermétiquement isolées de tout autre cabinet.** Chaque cabinet dispose d'une base de données privée.
- **Certification ISO 27001** de l'ensemble des processus et procédures opérationnelles de Wolters Kluwer concernant l'infrastructure, l'assurance qualité et le support niveau 3.

Aujourd'hui, ce sont plus de 11 000 utilisateurs qui hébergent quotidiennement leurs données sur nos serveurs. Merci de leur confiance !

Découvrez nos logiciels de gestion : wk-logiciels.fr

McAfee SECURE · Norton SECURED powered by Symantec · ISO 27001 Certified

Wolters Kluwer

SÛRETÉ NUMÉRIQUE AU SEIN DES CABINETS D'AVOCAT : ENJEUX ET MÉTHODES

L'accélération de la transformation digitale a eu lieu à marche forcée, en raison de l'épidémie de Covid-19, pour l'ensemble des acteurs du monde juridique et judiciaire. Dans le même temps, la menace numérique s'est diversifiée et amplifiée : cyberattaques, cybermalveillance et désinformation se sont intensifiées[1]. Les avocats n'ont échappé ni à l'un, ni à l'autre. Les risques sont bien réels, quelles que soient la taille du cabinet et la nature des dossiers traités. C'est l'une des raisons pour lesquelles la Rédaction du Journal du Village de la Justice a décidé de se pencher sur une partie des outils et méthodes permettant de garantir, dans le cyberespace, la confidentialité des données et informations qu'ils détiennent et qu'ils se doivent de protéger. Effectivité du secret professionnel, responsabilité civile professionnelle (RCP) et positionnement du praticien en tant que partenaire de confiance, les enjeux de la cybersécurité et de la cyberrésilience sont multiples pour les avocats. Quoi, pourquoi et comment se préoccuper du risque cyber et adopter une approche raisonnée de la sûreté numérique au sein des cabinets, on vous dit tout[2].

Les habitudes professionnelles ont changé sur de très nombreux aspects. Il est désormais acquis que le numérique s'installe profondément et durablement dans l'esprit et la pratique des avocats. Et, ce, qu'il s'agisse de travailler au quotidien sur les dossiers, au bureau, en télétravail ou en mobilité, de collaborer au sein des cabinets, d'échanger avec les juridictions et les confrères, de communiquer avec la clientèle et les partenaires, de se doter d'outils d'automatisation, d'aide à la décision et de solutions de paiement en ligne, de gérer son e-réputation sur les réseaux sociaux ou bien encore de s'informer.

Les enquêtes et les discussions sur la digitalisation des cabinets[3] le montrent néanmoins, la profession ne s'est, globalement, pas encore complètement emparée de la question de la sécurité dans l'usage du numérique, même si la situation semble évoluer. Les avocats se sentent concernés par la cybersécurité : 93% d'entre eux n'évaluent pas les risques cyber comme étant mineurs pour leur activité[4]. Pour autant, la sécurité dans les échanges numériques n'est une préoccupation que pour un avocat sur sept ; 92 % des praticiens concèdent ne pas connaître ou n'avoir pas une bonne connaissance du chiffrement des données[5]. Avec la crise sanitaire, nécessité faisant loi, il n'est donc pas certain que l'évolution des pratiques digitales de la profession ait été assortie d'une pleine et entière prise de conscience des risques actuels et à venir auxquels les cabinets d'avocat sont exposés. Ici comme ailleurs, au-delà de la simple sensibilisation et du bon sens individuel, la mise en place de mesures adéquates de cyberprotection reste insuffisante. Responsabilité partagée probablement, faute peut-être de savoir exactement quoi faire et par où commencer, à qui s'adresser et quels outils utiliser…[6] Il est donc temps de passer de la simple préoccupation à la pratique !

1 - Voir Sénat, 10 juin 2020, Suivi de la cybermenace pendant la crise sanitaire, Rapp. d'information n° 502 ; Interpol, août 2020, Rapport d'évaluation mondial portant sur la cybercriminalité liée au COVID-19 (www.interpol.int).
2 - Ce dossier, rédigé après échanges avec des experts en cybersécurité, est générique et n'entend pas prendre en considération la situation particulière de chaque cabinet.
3 - Voir notamment « *Cybersécurité des cabinets d'avocats : il est urgent et assez simple de s'en préoccuper* » (www.village-justice.com, article n° 35980 ; compte-rendu des e-débats du CNB du 25/06/2020).
4 - Bilan numérique des avocats 2020, à paraître sur www.village-justice.com.
5 - *Ibid*.
6 - Sur ce point, voir « *Et si la cybersécurité devenait enfin accessible aux petites et moyennes structures d'exercice ?* », Entretien avec F. Imbert-Vier, dans ce numéro du Journal du Village de la Justice, p. 32.

SCB
SOCIETE DE COURTAGE
DES BARREAUX

www.scb-assurances.com

L'assurance Cyber-Risques

L'assurance Cyber-Risques à partir de 29 €/mois TTC*

- Souscription simplifiée jusqu'à 250 000 € de garantie
- Pas de redondance avec les garanties RC professionnelles
- Couvertures : atteintes aux systèmes d'informations, fraudes et tentatives d'extorsions
- Prise en compte des contraintes RGPD (notifications, enquêtes CNIL…)
- Assistance 24h sur 24, 7 jours sur 7

Pour des garanties plus élevées et au-delà de 19 avocats, la SCB vous proposera une étude personnalisée.

Détails https://www.scb-assurances.com/fr/cyber-risques

* Pour un cabinet de moins de 10 avocats

SCB : 47 bis D Bd Carnot • CS 20740 • 13617 Aix-en-Provence cedex 1
Tél. : 04 13 41 98 30 • contact@scb-assurances.com

La réflexion relative à la digitalisation des cabinets est encore, le plus souvent, focalisée sur la question de l'acquisition d'outils de production et de gestion des structures d'exercice. Souhaiter gagner en productivité grâce aux facilités du numérique et/ou décider d'externaliser certaines activités ou fonctions du cabinet est, bien entendu, tout à la fois légitime et louable. C'est même souhaitable, en ce que cela permet au praticien notamment de se concentrer sur des tâches à plus forte valeur ajoutée. Mais comme le souligne l'ANSSI[7], « *le développement technologique rapide associé à l'intégration systématique de moyens informatiques de plus en plus complexes et interconnectés rendent les systèmes (…) à la fois beaucoup plus performants et plus vulnérables* »[8]. C'est la raison pour laquelle nous avons choisi de réfléchir à la cybervulnérabilité des cabinets d'avocat.

Les cyberattaques se multiplient. Les chiffres et statistiques sont pourtant aujourd'hui insuffisants – pour ne pas dire inexistants – pour quantifier le phénomène en ce qui concerne spécifiquement les cabinets d'avocat et, plus largement d'ailleurs, les professionnels du droit. Mais tout comme d'autres cas plus anciens[9], les fuites de données lors de l'affaire des *Panama Papers*[10], l'attaque subie par le cabinet américain *Grubman Shire Meiselas & Sacks*[11] ou la perte d'une clé USB contenant une copie des actes d'enquête sur les attentats terroristes de 2015[12] font figure d'exemples. Les dégâts causés par le rançongiciel Maze[13] et l'attaque, massive, du parquet de Paris et d'autres magistrats et avocats en charge d'affaires « *sensibles* »[14] le montrent : les cabinets d'avocat, indépendamment de leur taille et de leur spécialité, sont bien loin d'être à l'abri de la cybermalveillance ; ils en deviennent même une cible privilégiée. Nous avons donc cherché à comprendre les raisons de cette exposition particulière des avocats et de voir comment pallier, autant que faire se peut, cette vulnérabilité.

« Les cabinets d'avocat, indépendamment de leur taille et de leur spécialité, sont bien loin d'être à l'abri de la cybermalveillance ; ils en deviennent même une cible privilégiée ».

Qu'est-ce qui rend les cabinets d'avocats vulnérables aux menaces émanant notamment du cyberespace ? La réponse est la même que pour les autres organisations : les données et informations dont ils disposent. Ou, plus exactement, leur confidentialité et, partant, leur valeur. Mais la spécificité ici est que l'avocat est le « *confident nécessaire* »[15] de son client. Il détient donc, nécessairement, un grand nombre de données et d'informations relatives à ce dernier. Il en a connaissance *ès* qualités, en raison même de l'exercice de sa profession. La seconde particularité est que ces données et informations sont protégées par l'obligation légale et déontologique forte qu'est le secret professionnel. Et c'est parce qu'« *il est de la nature même de la mission de l'avocat qu'il soit dépositaire des secrets de son client et destinataire de communications confidentielles* »[16], qu'il constitue une cible privilégiée de la cybermalveillance. **Par l'intermédiaire de l'avocat, il est en effet possible d'accéder, en un seul lieu, à une multitude d'informations qui ne sont généralement pas accessibles (ou sont éparpillées) ailleurs.** La cybervulnérabilité des cabinets d'avocat est donc inhérente à l'activité même de la profession, ce qui justifie l'importance de préserver ce sanctuaire, en le protégeant des menaces émanant du cyberespace.

Les risques dans ce domaine sont réels et diversifiés : piratage, surveillance, fraudes diverses. Leurs conséquences sont presque immanquablement dommageables, voire hautement préjudiciables. Elles se réalisent aux dépens du praticien lui-même, en termes financiers, de capacités opérationnelles et de réputation notamment ; elles se produisent aussi au détriment de ses clients ainsi exposés[17]. « *Le risque numérique qui pèse chaque jour davantage sur les organisations peut [en effet] aller jusqu'à mettre en péril leur survie et celle de leurs parties prenantes* »[18]. À l'inverse, une bonne gestion de la sécurité des outils numériques et la sécurisation des flux d'informations au sein du cabinet est un marqueur fort de professionnalisme, de nature à rassurer objectivement le client quant à la garantie de confidentialité des données et informations confiées ou créées. Et l'on comprend alors aisément l'affirmation selon laquelle **la protection du secret professionnel passe nécessairement par le renforcement de la sécurité informatique des avocats**[19].

7 - Agence Nationale de la Sécurité des Systèmes d'Information.
8 - Édito de G. Poupard, Directeur général de l'ANSSI, sur le site de l'Agence (www.ssi.gouv.fr).
9 - Voir par ex. à Orléans, Poitiers et Saint-Raphaël en 2016 (« *Comment ce cabinet d'avocats a été victime d'une cyberattaque* », par G.D., pour Var Matin, 21 janv. 2016 ; « *Une cyberattaque lancée contre un cabinet d'avocats d'Orléans* », par P. Renaud pour La République du Centre, 5 oct. 2016 ; « *Un cabinet d'avocats frappé par une cyberattaque* », par E.C., pour La Nouvelle République, 17 oct. 2016).
10 - Voir notamment « *Que doit-on retenir comme enseignement de l'affaire des Panama Papers ?* », B. Jacq, 12 avr. 2019 (https://infoguerre.fr).
11 - Voir « *Le célèbre cabinet d'avocats Grubman Shire Meiselas & Sacks victime de pirates informatiques* », par M. Untersinger pour Le Monde, 15 mai 2020.
12 - « *Charlie Hebdo. Une clé USB disparaît : grosse boulette des avocats* », Ouest France, 23 août 2016.
13 - Voir notamment « *BTP, cabinet d'avocats : Maze revendique deux nouvelles victimes en France* », par V. Marchive, pour LeMagIT, 2 sept. 2020.
14 - Voir « *Le Tribunal de Paris a été la cible d'un piratage informatique massif* », par P. Ceaux, pour Le Journal du Dimanche, 6 sept. 2020 ; « *Plusieurs magistrats et avocats touchés par une attaque informatique, une enquête ouverte* », Le Monde avec AFP, 6 sept. 2020.
15 - Art. 2.1 du RIN (Règlement Intérieur National de la profession d'avocat).
16 - Art. 2.3.1 du Code de déontologie des avocats européens.
17 - Particulièrement s'il s'agit d'actions de surveillance au profit de la partie adverse ou de déstabilisation et/ou d'ingérence économique dans les affaires d'un concurrent.
18 - ANSSI & AMRAE, nov. 2019, Maîtrise du risque numérique. L'atout confiance (www.ssi.gouv.fr).
19 - Conseils et Recommandations du Conseil des barreaux européens (CCBE) pour le renforcement de la sécurité informatique et la protection du secret professionnel des avocats contre la surveillance illégale (mai et déc. 2016 ; www.ccbe.eu).

« La cybervulnérabilité des cabinets d'avocat est inhérente à l'activité même de la profession ».

La cybersécurité est l'« *état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles* »[20]. Mais aux termes-mêmes du Règlement européen sur la cybersécurité, celle-ci « *n'est pas qu'une question liée à la technologie, mais une question pour laquelle le comportement humain est tout aussi important* »[21]. La vulnérabilité s'entend en effet d'une « *faute, par malveillance ou maladresse* », non seulement « *dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système* », mais aussi « *dans la façon de l'utiliser* »[22]. La complétude de cette définition permet de comprendre l'étendue des actions à réaliser pour assurer la sûreté numérique des cabinets d'avocat. Elles comportent deux volets : l'un est technique (la cybersécurité au sens strict) et concerne la protection des outils numériques et des réseaux et systèmes d'informations ; l'autre est social et comportemental (la cyberrésilience au sens large) et renvoie à des problématiques d'accompagnement et de sensibilisation de l'utilisateur ou du détenteur de l'information.

Cette sûreté numérique est au cœur de multiples enjeux pour les praticiens. Mais deux constats doivent être faits. D'une part, celui selon lequel toutes les données et informations n'ont pas toutes besoin du même degré de protection dans le cyberespace, alors même qu'elles sont, toutes, protégées au titre du secret professionnel. « *Les mesures prises pour sécuriser un environnement doivent être proportionnelles à la valeur de l'objet de cette sécurisation* »[23]. D'autre part, celui selon lequel le risque zéro n'existe pas : la protection parfaite des systèmes d'information et le secret absolu sont impossibles à atteindre.

20 - Glossaire de l'ANSSI, accessible sur le site internet de l'Agence (https://www.ssi.gouv.fr/entreprise/glossaire).
21 - Cons. 8, Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (JOUE L 151/15, 7 juin 2019).
22 - Glossaire de l'ANSSI, « Vulnérabilité » (www.ssi.gouv.fr)
23 - OTAN, 2016, Cybersécurité - programme de référence générique, Entérinement du programme de référence pour la cybersécurité, élaboré par le groupe de travail sur les défis de sécurité émergents du Groupement PPP (www.nato.int).

Les menaces évoluent quotidiennement et s'y adapter rapidement suppose un immense travail de veille et de sécurisation, ainsi qu'un budget dédié tout aussi considérable. Services que très peu de structures d'exercice, il faut bien le reconnaître, sont en mesure de mettre en place ou de s'offrir. Il ne s'agit donc pas de transformer les cabinets en immenses forteresses numériques, état peu compatible d'ailleurs avec le quotidien même de l'avocat. Mais c'est sur cet équilibre que repose une démarche "cybervertueuse" : ce sera d'abord comprendre et reconnaître sa vulnérabilité. Ce sera ensuite, selon une logique à la fois proactive et réactive, mettre en place les mesures *ad hoc*, indispensables pour prévenir les incidents de cybersécurité. Ce sera enfin être cyberrésilient, afin de permettre la poursuite et la reprise de l'activité – en somme, de rester opérationnel – en dépit de l'incident. Et tout ceci amène à examiner la manière dont les avocats peuvent démontrer qu'ils ont réfléchi à la question.

« *Loin de vouloir effrayer, la juste voie en la matière est bel et bien d'informer, de démystifier et de responsabiliser afin d'influencer positivement la prise de décision* »[24]. L'idée, avec ce dossier sur la sûreté numérique des cabinets d'avocat, n'est évidemment pas d'adopter un discours moralisateur et conduisant à devenir obsessionnel et à tout « *cadenasser* ». Il s'agit de contribuer à ce que les avocats soient en mesure de se forger un avis éclairé sur les enjeux et les menaces auxquels ils sont confrontés dans le cyberespace.

Pour appréhender ces aspects spécifiques de la gouvernance de l'information au sein des cabinets d'avocat, nous vous proposons de procéder en quatre temps. La **première étape** consiste à se concentrer sur l'origine de la vulnérabilité des cabinets d'avocat, en faisant une sorte d'état des lieux de toutes les données et informations qu'ils détiennent et en déterminant celles qui, parce qu'elles sont critiques, doivent faire l'objet de mesures de protection renforcées. La **deuxième étape**, avec un niveau de complexité se voulant volontairement abordable, porte l'idée que la sûreté numérique doit devenir un sujet stratégique de la gestion du cabinet. Ceci, en se préoccupant à la fois des menaces auxquels les avocats sont exposés et en envisageant la manière de réagir à un incident de cybersécurité. La troisième étape de notre démarche repose sur la visualisation de l'intérêt – des intérêts devrions-nous plutôt dire – pour les praticiens d'évaluer et de réduire le risque cyber au sein de leurs structures. **La quatrième et dernière étape**, à paraître dans le prochain numéro du Journal du Village de la Justice, nous conduira à envisager, de manière plus pragmatique, la mise en place des mesures d'« *hygiène numérique* » au sein des structures d'exercice.

24 - Guide ANSSI-DACG, sept. 2020, Attaques par rançongiciels, tous concernés. Comment les anticiper et réagir en cas d'incident ?, Édito.

Au sommaire de ce dossier

Partie 1. Les données et informations détenues par les cabinets d'avocat : que faut-il protéger ?

La multiplicité et l'hétérogénéité des données et informations que l'avocat recueille ou crée dans l'exercice de ses fonctions, ainsi que la diversité de leurs supports rendent presque illusoire d'en établir une liste exhaustive. Il est en outre patent que toutes les données et informations détenues par les avocats n'ont pas le même besoin de protection. Il faut donc faire un état des lieux **du « *patrimoine* » informationnel du cabinet** et identifier ce qu'il faut protéger en priorité.

En parallèle de l'identification du contenu lui-même, il importe aussi de **préciser la localisation des données et informations**, c'est-à-dire notamment le support sur lequel elles sont stockées : ordinateurs fixes ou portables, tablettes, serveurs informatiques, supports informatiques amovibles (disque dur, clé USB, carte mémoire, etc.), dossiers papier, logiciels, etc. Pour parfaire le travail d'inventaire, il faudra **préciser l'identité des personnes pouvant accéder auxdites données et informations.**

1.1. Recenser les données et informations relatives aux personnes physiques et morales

Les données et informations détenues par les cabinets d'avocat portent sur son activité propre (propriété intellectuelle, savoir-faire, personnels, etc.) et sur ses clients (données personnelles, contrats, projets, etc.). Sont en effet concernées, toutes les « *informations et confidences* »[25] reçues par l'avocat, ainsi que les données qu'il collecte et traite dans l'exercice de la profession, en toute matière (conseil ou contentieux) et quels qu'en soient le support et l'état (stockage, traitement ou circulation). Il n'en reste pas moins possible de tenter de les recenser au regard de leur objet, selon une démarche en deux temps, d'inventaire et de qualification, comparable à celle requise par la mise en conformité avec les obligations découlant du RGPD[26].

En ce qui concerne les **données et informations relatives aux personnes physiques**, un premier recensement est possible à la simple lecture du RGPD, qui aborde la question du droit fondamental de protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel. Rappelons que la donnée personnelle est définie comme toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant[27]. Entrent ainsi dans cette catégorie les données relatives à l'état civil et l'identité (nom, prénom(s), date de naissance, lieu de naissance, domicile…), le numéro de Sécurité sociale (NIR), la voix et l'image, les informations relatives à la vie personnelle (résidence, situation familiale, habitudes de vie…) et professionnelle (courriel, adresse professionnelle…) et à la situation économique et financière (revenus, situation bancaire et fiscale…), les données d'identification (numéros clients, téléphone, plaque d'immatriculation…), de connexion (adresses IP, logs…) ou bien encore les données de localisation (données GPS, GSM…). Quant à la catégorie particulière des données personnelles que sont les

25 - Comp. art. 2.2 du RIN, relatif au secret professionnel.
26 - Règlement Général sur la Protection des Données : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE (JOUE L 119/1, 4 mai 2016).
27 - RGPD, art. 4.1.

données dites sensibles, elles sont relatives à l'origine ethnique, la nationalité, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale. S'y ajoutent les données génétiques et biométriques, celles concernant la santé, la vie ou l'orientation sexuelle[28], ainsi que celles relatives aux procédures et antécédents judiciaires. Lorsqu'ils concernent les clients (ainsi que, le cas échéant, la ou les parties adverses), ils sont notamment mentionnés et exploités dans les actes de procédure[29], joints en tant que pièces justificatives, contenus dans les fichiers clients des cabinets, les conventions d'honoraires et factures, ou bien encore collectées lors de la visite du site internet du cabinet par un internaute. Lorsqu'ils concernent les associés, collaborateurs et salariés du cabinet, ces éléments sont notamment utilisés dans le cadre des opérations RH et paie, des déclarations fiscales, du règlement des cotisations, du versement des fonds, de l'accès aux interfaces, portails et réseaux virtuels professionnels, etc. La matière est, pour le moins, très large, tant sur le fond que sur la forme.

En ce qui concerne **les données et informations relatives aux personnes morales**, le recensement peut sembler plus complexe, ne serait-ce que parce que le RGPD ne les concerne que par la protection attachée aux données personnelles des personnes physiques la composant. Il n'existe donc pas, en tant que telle, d'énumération "officielle" pouvant servir de base à leur recensement. Quoi qu'il en soit, les personnes morales disposent notamment d'un droit à la protection de leur nom, de leur domicile, de leurs correspondances et de leur réputation[30] et ces éléments doivent donc entrer dans le champ de la réflexion sur la sûreté numérique du cabinet. Plus encore, les données et informations relatives à leur forme, leur dénomination, leur siège social, leurs numéros d'immatriculation (SIREN, SIRET, Code NAF), le montant et la devise du capital social, l'objet social et l'activité détaillée de l'entreprise, le sigle et l'enseigne, l'organe qui les représente légalement, etc. sont autant d'informations recueillies et traitées par les cabinets d'avocat. S'y ajoutent celles relatives aux fichiers clients ou fournisseurs, les organigrammes, les études marketing et de marché, les politiques de prix, les accords commerciaux, les politiques de recrutement et de rémunération, le savoir-faire technique ou technologique (secrets de fabrique, brevets, dessins et modèles, algorithmes, etc.), les bilans financiers et données comptables, les business plan et notes de stratégie, les réponses à appel d'offre ou les données et informations issues de la surveillance des locaux (vidéosurveillance, badge etc.). En somme, il s'agit des éléments relatifs au fonctionnement habituel de l'entreprise cliente, qu'ils soient ou non couverts par le secret des affaires[31] et dotés ou non d'une valeur commerciale intrinsèque. Ils constituent la matière avec laquelle travaillent les avocats accompagnant les personnes morales, sans compter, bien sûr, celles concernant les cabinets eux-mêmes. Ici encore, on le constate, le domaine est bien vaste.

« Il faut faire un état des lieux du « patrimoine informationnel » et identifier ce qu'il faut protéger en priorité ».

La plupart des données et informations à la disposition des avocats relèvent, avec certitude, de la vie privée des clients personnes physiques ou des intérêts légitimes et du secret économique des clients personnes morales. On le sait, **tous ces éléments sont, peu ou prou, utilisés au quotidien par les cabinets d'avocat ; plus encore, ce sont des éléments indispensables à l'exercice de leurs missions.** Mais les besoins en sécurité varient selon les informations et données confiées ou créées par les cabinets d'avocat. Certaines peuvent, sans risque, être connues ; d'autres doivent, au contraire, bénéficier d'une protection particulière, en tenant compte de ce que leur confidentialité protège et au vu des conséquences que leur divulgation (par hypothèse, non souhaitée) génèrerait. Une fois que l'inventaire des contenus informationnels des cabinets d'avocat a été réalisé, une approche "cyber vertueuse" de la gestion de l'information doit conduire à *qualifier* ces données et informations, pour identifier celles qui, parce qu'elles sont critiques, doivent faire l'objet d'une protection renforcée.

28 - RGPD, cons. 51.
29 - Voir par exemple les articles 54 et 59 du Code de procédure civile, relatifs aux mentions obligatoires des actes introductifs d'instance.
30 - Cass. 1re civ., 17 mars 2016, n° 15-14.072, Bull. civ. I, n° 67.
31 - Au sens des articles L. 151-1 et suivants du Code de commerce, créés par la loi n° 2018-670 du 30 juillet 2018 (JO 31 juill.) relative à la protection du secret des affaires, et de la Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (JOUE L 157/1, 15 juin).

1.2. Qualifier les « informations critiques » confiées ou créées par les cabinets

Par principe, les informations détenues par les avocats, « *confidents nécessaires* » de leurs clients, ont, toutes, vocation à être couvertes par le secret professionnel. L'utilisation de ces informations par l'avocat relève de sa responsabilité. Mais **dans le cyberespace, c'est précisément cette garantie de confidentialité et l'opposabilité du secret qui posent problème, les menaces pesant sur les cabinets ayant exactement pour effet, ou pour objet, de les priver de la maîtrise des flux d'information.** C'est pourquoi un niveau minimal de sécurité numérique doit être instauré au sein des cabinets. Toutes les données et informations confiées ou créées par l'avocat n'ont pas besoin d'être, sur le plan informatique, sécurisées de la même façon. La logique est ici la même que celle qui conduit à admettre que tous les documents ou objets possédés par une personne n'ont pas besoin d'être placés dans un coffre-fort ou que toutes les zones d'un bâtiment n'ont pas besoin d'être couvertes par la vidéo-surveillance.

« *Une information protégée n'est pas nécessairement une information cadenassée* »[32] et protéger de manière inconditionnelle, l'intégralité des données et informations détenues par les cabinets conduirait à en faire de véritables forteresses digitales, peu compatibles, il faut bien en convenir, avec l'exercice même de l'activité (procédures trop contraignantes, trop complexes, trop coûteuses). Il faut, avec discernement, identifier, parmi toutes les informations confidentielles détenues par les cabinets, celles qui doivent être considérées comme « *sensibles* », voire « *critiques* » et sur lesquelles pèsent, de ce fait, des obligations de confidentialité et de sécurisation renforcées.

> ***« Il faut, avec discernement, identifier, parmi les informations confidentielles, celles qui doivent être considérées comme sensibles, voire critiques ».***

Parmi les données et informations dont le niveau de cyberprotection doit être renforcé, on trouve indiscutablement les **données qualifiées de « *sensibles* » par le RGPD** : leur révélation et leur utilisation sans le consentement de la personne physique concernée génère, par nature, une atteinte aux droits fondamentaux. Le travail de cartographie des traitements de données à caractère personnel réalisé pour la mise en conformité avec le RGPD, peut donc être utilement ré-exploité dans le cadre des démarches de cybersécurité. Mais la qualification d'information à protéger de manière renforcée dans le cyberespace s'applique bien au-delà. La sensibilité et la criticité des informations confidentielles (i.e. celles qui sont couvertes au titre du secret professionnel de l'avocat) peuvent être déterminées notamment par rapport aux conséquences dommageables que sa « *compromission* » pourrait avoir[33] : si elles venaient à être divulguées ou utilisées sans autorisation, alors qu'elles avaient vocation à rester confidentielles, voir secrètes, de nombreux impacts pourraient être subis tant par le client, que par le cabinet lui-même (continuité des activités, réputation, conséquences juridiques et financières[34]).

Outre cette analyse au regard des conséquences probables – et peut-être même préalablement –, **il faut raisonner par rapport à l'utilité de l'information**. Peut ainsi être qualifiée de « *sensible* » ou de « *critique* », l'information dite « *utile* »[35] pour le client, c'est-à-dire celle qui est nécessaire à son fonctionnement quotidien et celle nécessaire à sa prise de décision stratégique (par exemple dans le cadre d'une négociation commerciale ou dans un contexte judiciaire). « *La valeur de ce patrimoine, dit informationnel, peut en effet être appréciée au regard des opportunités qu'il offre quand on l'utilise correctement et des conséquences négatives dans le cas contraire* »[36]. C'est ce qui explique que ces informations n'ont pas vocation à être rendues publiques

32 - « *Information sensible d'entreprise : une attention de tous les instants* », C. Gengembre, Tribune, Les Echos, 14 mars 2018.

33 - Cette évaluation est celle qui se fait notamment dans le cadre de l'analyse des risques (risk management), selon des scénarios de menaces plus ou moins réalistes et avec des degrés d'appréciation plus ou moins flexibles selon la structure concernée. Si le besoin de confidentialité est important dans l'évaluation des risques liés à la cybermalveillance, il n'est pas le seul : il faut également de prendre en considération la question de la disponibilité (il est possible d'y accéder en temps voulu) et d'intégrité (la modification ne se fait qu'en raison d'une action volontaire et autorisée) des données et informations.

34 - Sur les impacts d'un cyber incident, voir *infra*, § 3.1.

35 - Plus précisément, l'information utile est « *celle dont ont besoin les différents niveaux de décision de l'entreprise ou de la collectivité, pour élaborer et mettre en œuvre de façon cohérente la stratégie et les tactiques nécessaires à l'atteinte des objectifs définis par l'entreprise dans le but d'améliorer sa position dans son environnement concurrentiel* » (Intelligence économique et stratégie des entreprises, Travaux du groupe de travail présidé par Henri Martre, La documentation française, févr. 1994).

36 - EBIOS 2010, Méthode de gestion des risques (www.ssi.gouv.fr). L'EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est une méthode élaborée notamment par l'ANSSI permettant d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information (SSI). Une nouvelle version a été établie en 2018 (EBIOS Risk Manager).

de manière aléatoire ; certaines doivent d'ailleurs impérativement rester secrètes, ne serait-ce que temporairement. C'est aussi ce qui explique que l'évaluation de la sensibilité et de la criticité des informations détenues par les cabinets d'avocat ne peut pas être prédéterminée : elle doit se faire *in concreto*, selon une échelle qui est propre à chaque cabinet et à chaque client[37].

La prise de connaissance de l'identité d'un client ou d'une référence de dossier, n'a pas, ne serait-ce qu'intuitivement, le même degré de criticité que l'information sur l'état de cessation des paiements d'un client, sur l'intention d'engager une action en justice ou bien encore sur un projet de fusion-acquisition, de divorce ou de plan social. Les informations couvertes par le secret de l'enquête et de l'instruction, celles sur l'état de santé d'un dirigeant social ou les coordonnées bancaires doivent faire l'objet d'une appréciation encore différente. Il en est de même de celles relatives à l'existence de pratiques illégales ou contraires à l'éthique, des secrets de fabrication ou bien encore des bases de données clients-fournisseurs.

« Plus les conséquences de la compromission de l'information risquent d'être graves, plus les mesures de protection doivent être renforcées ».

Cette analyse de la criticité des informations est essentielle. Elle doit être menée et affinée, rappelons-le, à la fois par rapport au cabinet lui-même et pour chaque client. Le travail de recensement/localisation et de qualification doit être aussi précis et aussi exhaustif que possible. Il est en effet certain que plus les conséquences de la compromission de l'information risquent d'être graves, plus les mesures de protection doivent être renforcées, pour que leur confidentialité soit assurée. Ce n'est donc qu'au terme d'une démarche préalable, rationnelle et précise d'identification des ressources à protéger, qu'il devient possible d'engager, de manière raisonnée, la réflexion sur les mesures de protection à adopter. Mais encore faut-il, il est vrai, savoir contre quoi et comment se protéger.

37 - La révélation d'une information pourrait avoir un impact minime pour un client, mais celle de l'information de même nature à propos d'un autre client pourrait être génératrice de conséquences dommageables pour ce dernier. Tout dépendra aussi de l'intention de la personne en prenant indument connaissance.

Partie 2. La cyberrésilience des cabinets d'avocat : quelles réactions face à quelles menaces ?

Inventorier le patrimoine informationnel du cabinet est une première étape importante dans la construction de la sûreté numérique du cabinet, tout comme la mise en place de mesures de bonnes pratiques d'hygiène informatique, que nous aborderons un peu plus loin. Ces actions sont nécessaires, mais elles ne suffisent malheureusement pas à garantir, dans le cyberespace, la confidentialité des informations et données détenues ou créées par les avocats. Il ne s'agit pas seulement de sécuriser les outils et systèmes informatiques et leur utilisation, mais aussi de protéger toute l'activité du cabinet, en lui permettant d'affronter efficacement une cyberattaque ou, plus largement, une fuite ou une altération de données. Et tels sont précisément les objets de la cybersécurité et de la cyberrésilience, qui doivent devenir un impératif pour les cabinets d'avocat. Prendre la mesure du risque numérique et s'organiser pour y faire face est une démarche progressive. Il est certain que l'on ne devient pas cyberrésilient du jour au lendemain ! Mais pour être en mesure de gérer l'insécurité numérique du cabinet, il faut être prêt, le cas échéant, à changer de paradigme et à modifier ses habitudes. À cet égard, il est possible et judicieux de commencer par s'informer sur les menaces émanant du cyberespace[38] et à se préparer à devoir réagir à un incident cyber.

2.1. S'informer sur les menaces

Impossible, aujourd'hui, de nier l'ampleur du phénomène : les incidents cyber sont en augmentation croissante. Le constat fait en 2018 selon lequel « *il ne se passe pas une semaine sans qu'une nouvelle affaire nous rappelle que le cyberespace est miné par des risques qui lui sont spécifiques* »[39] est encore plus vrai aujourd'hui. « *Chacun d'entre nous, dans son environnement proche, a déjà été témoin ou victime de la concrétisation de la menace* »[40]. Celle-ci ne fléchît pas, bien au contraire, elle se renforce et se diversifie : « *la cybercriminalité évolue à un rythme effréné, et de nouvelles tendances ne cessent d'apparaître* »[41].

Les cybermenaces sont multiples. Utilisation illégale d'un mot de passe, vol ou perte d'équipements informatiques, logiciels malveillants et virus informatiques, hameçonnage, écoutes téléphoniques illégales, piratage d'objets connectés, comportements négligents et à risques ne sont, malheureusement, qu'une partie des cas auxquels les cabinets d'avocat peuvent, comme les autres organisations, être confrontés. Impossible donc d'en établir une liste exhaustive, tant leur variabilité est grande. Ajoutons, il faut bien admettre en toute humilité, qu'en raison de la technicité des moyens employés et du jargon utilisé, il est parfois assez difficile de s'y retrouver pour le non-spécialiste. Mais comme le souligne le Conseil des Barreaux Européens (CCBE), non seulement « *il peut s'avérer nécessaire aux avocats d'investir dans des systèmes de sécurité informatiques, des outils de protection et des outils de chiffrement, mais il est également nécessaire pour y parvenir que l'avocat ait une bonne connaissance de l'environnement dans lequel ces outils évoluent* »[42].

Indépendamment des motivations des cybercriminels (financières, idéologiques, reconnaissance sociale, espionnage industriel, surveillance, déstabilisation par atteinte à l'image et la réputation ou par sabotage) et des évolutions de leurs profils, il peut être admis que les actes de cybermalveillance sont, au sens

38 - Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques (ANSSI, Glossaire, « *Cyberespace* », www.ssi.gouv.fr).
39 - Conseil général de l'économie, janv. 2018, La cyber résilience, Rapp. n° 2017/02/CGE/SR (www.economie.gouv.fr).
40 - *Ibid*.
41 - Interpol, Infractions, Cybercriminalité (www.interpol.int).
42 - CCBE, 2016, Conseils pour le renforcement de la sécurité informatique des avocats contre la surveillance illégale (www.ccbe.eu).

large, des actions tentées ou commises *contre* ou *grâce* aux outils, systèmes et infrastructures informatiques et numériques. Sans entrer dans un examen détaillé et exhaustif des différentes menaces pesant sur les données et informations détenues par les cabinets d'avocat, il est possible de retenir quelques idées directrices pour appréhender la matière[43].

Il faut avoir conscience que la source des menaces est diversifiée : ces dernières peuvent être techniques ou humaines, externes ou internes à la structure, sachant que près d'un incident pour trois est d'origine humaine et interne. Dans tous les cas et comme pour les autres organisations, les besoins en cyberprotection se mesurent en termes de confidentialité[44], de disponibilité[45] et d'intégrité[46] des données et informations[47]. Tels sont précisément le rôle et la finalité des audits techniques et organisationnels de cybersécurité : déterminer, avec précision et réalisme, si le cabinet est ou non exposé à chacune des sources de menaces, dans quelles proportions et de mesurer les risques afférents[48].

« La source des menaces est multiple : ces dernières peuvent être techniques ou humaines, externes ou internes à la structure ».

Du côté des **menaces d'origine humaine**, deux idées seraient principalement à retenir : d'une part, le fait que les personnes à l'origine de l'incident peuvent agir de façon intentionnelle ou accidentelle ; d'autre part, le fait que l'auteur de l'incident peut disposer de plus ou moins grandes capacités de nuisances selon notamment son expertise, ses ressources, le temps dont il dispose, ainsi que ses possibilités d'accès et d'action sur le système d'information.

En découle une distinction entre les sources humaines agissant de manière délibérée et les sources humaines agissant de manière involontaire, avec, dans les deux cas, l'application de critères complémentaires : internes ou externes, avec de faibles capacités, avec des capacités importantes ou des capacités illimitées. Prenons des exemples. Le collaborateur malveillant, avec des possibilités d'action limitées sur le système d'information (personnel en fin de contrat ou voulant se venger de son employeur ou de ses collègues…) ou le client désirant obtenir indûment des avantages peuvent, selon les circonstances, être considérés comme des « *sources humaines internes, malveillantes, avec de faibles capacités* ». Le cabinet pourrait ici être particulièrement confronté à des fuites d'informations. En revanche, le collaborateur maladroit ou inconscient, les personnels à faible conscience d'engagement, peu sensibilisés ou peu motivés dans leur relation contractuelle avec la structure entreront dans la catégorie des « *sources humaines internes, sans intention de nuire, avec de faibles capacités* ». S'il s'agit d'un administrateur système ou réseau ou d'un dirigeant agissant par vengeance, la qualification pourra être celle d'une « *source humaine interne, malveillante, avec des capacités illimitées* ». Un militant idéologique ou politique malintentionné ou un pirate informatique passionné mais non expert, les concurrents, etc. pourront, eux, être qualifiés de « *sources humaines externes, malveillantes, avec des capacités importantes* ». Et l'on retrouvera ici notamment les risques de sabotage et d'espionnage, qui sont non seulement les pires cas de figure, mais aussi les plus difficiles à détecter. La démotivation au travail et la rupture des relations professionnelles sont assurément des situations particulièrement à risque pour la préservation de la confidentialité, de la disponibilité et de l'intégrité des données et informations détenues par le cabinet.

Du côté des **menaces d'origine technique**, elles peuvent également être internes ou externes à l'organisation, les attaques pouvant être réalisées à distance ou non. Concentrons-nous plus spécifiquement sur les menaces pesant particulièrement sur les outils digitaux (équipements informatiques, logiciels, canaux informatiques et de téléphonie), ainsi que sur les supports papier. Tous peuvent être détournés, espionnés, modifiés ou perdus, ce qui va également affecter la disponibilité, l'intégrité et la confidentialité des données et informations.

Le matériel peut être détourné, c'est-à-dire être utilisé à d'autres fins que celles prévues sans pour autant être modifié, ni endommagé. Mais les ressources de la structure peuvent, elles, être réduites ou rendues indisponibles. Il s'agira par exemple de l'usage d'un ordinateur ou d'une imprimante à des fins personnelles, du stockage de fichiers professionnels sur un ordinateur personnel ou de l'utilisation de matériels inadaptés à la sensibilité des informations stockées (disque dur, clé USB…). Un usage

43 - Nous sommes inspirés ici notamment des éléments de la base de connaissances EBIOS 2010 (précitée).
44 - Caractère réservé d'une information ou d'un traitement dont l'accès est limité aux seules personnes admises à la (le) connaître pour les besoins du service, ou aux entités ou processus autorisés (ANSSI, La cybersécurité des systèmes industriels, Méthode de classification et mesures principales, www.ssi.gouv.fr).
45 - Propriété permettant de rendre le service attendu en temps voulu et dans les conditions d'usage prévues (ANSSI, La cybersécurité des systèmes industriels, précité).
46 - Garantie que le système et l'information traitée ne sont modifiés que par une action volontaire et légitime (ANSSI, Glossaire, « *Intégrité* », www.ssi.gouv.fr).
47 - Ces propriétés répondent aux besoins en cybersécurité. S'y ajoute également un besoin en termes de traçabilité et de preuve, permettant d'identifier l'origine et de reconstituer le parcours d'un « *bien essentiel* » depuis sa production jusqu'à son utilisation (*ibid.*). L'idée est de pouvoir retrouver les circonstances dans lesquelles les données et outils ont évolué : traçabilité des actions menées, authentification des utilisateurs, imputabilité du responsable de l'action effectuée.
48 - Les informations mentionnées n'offrent naturellement aucune garantie quant à la sûreté de la protection et ne sauraient se substituer aux conseils et à l'accompagnement par un expert, qui fera une étude des risques (couplant les menaces, les vulnérabilités et l'analyse d'impact). Voir M. Meyer, « *L'audit cyber pour les cabinets d'avocats : comment et pour quoi faire ?* », Focus dans ce numéro du Journal du Village de la Justice, p. 34.

inapproprié des logiciels est également une menace pouvant conduire à la transformation des données (suppression, modification, déplacement), à la modification des accès, à un croisement d'informations dont le résultat est confidentiel ou à l'utilisation de canaux cachés pour traiter ou véhiculer des données discrètement (par exemple la stéganographie, qui permet de dissimuler des informations confidentielles au sein d'un message ordinaire ou l'exploitation de vulnérabilité dans le processeur d'un ordinateur, pour exécuter des opérations non souhaitées par l'utilisateur). Plus simplement, l'utilisation du verso d'impressions papier en tant que brouillons ou afin d'économiser le papier, aussi louable que soit cette intention, peut également mettre en péril la confidentialité des informations. Les attaques en « *déni de service* » (DoS pour *Denial of Service*) ont aussi pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu : un serveur est surchargé par l'envoi de multiples requêtes, une messagerie électronique est saturée par l'envoi d'une grande quantité de courriels à un même destinataire (*mail bombing*). On peut aussi y rattacher les pratiques de « *typosquatting* », qui consistent à déposer un nom de domaine très proche de l'adresse internet d'un autre site (par exemple avec un ou deux caractères différents), afin de capter une partie du trafic adressé sur un site officiel ; les plateformes de gestion des consultations d'avocats en ligne (avec éventuellement une solution de paiement en ligne) sont notamment exposées à ce type de cybermalveillance.

Le matériel peut être perdu par exemple lors d'un déménagement, d'un déplacement professionnel ou d'un envoi postal[49]. Dans ces hypothèses, le contenu n'est plus disponible pour la structure, mais le devient pour autrui, qui peut avoir des intentions malveillantes. On retrouve ici les cas de vol et de perte des outils informatiques et des supports papier (notes, dossiers, courriers, parapheurs, etc.). Sont également concernés, les situations de dons de matériel (ordinateur, périphérique ou autre support de données électroniques), de revente, de recyclage ou de mise au rebus d'un matériel obsolète : changer ses équipements informatiques sans s'assurer de la complète suppression des données (destruction physique, démagnétisation,…) comporte un risque important, puisque celles-ci, même effacées, restent souvent assez facilement récupérables. Les cas de « *disparition* » d'un logiciel en cas de non-renouvellement de licence ou de cession de droits sur une licence est à rapprocher de ces situations de perte. Les logiciels peuvent aussi être endommagés, partiellement ou totalement, temporairement ou définitivement en raison par exemple de l'effacement des codes sources ou de leur suppression par un code malveillant (bombe logique…).

Le matériel peut être modifié ou dégradé, par le retrait, l'ajout, la substitution ou la désactivation d'un élément. Il peut alors tomber en panne, dysfonctionner ou fonctionner autrement que dans le cadre de son usage normal. On trouvera ici notamment les cas de piégeage d'un matériel ou d'un logiciel contaminé par un programme ou code malveillant (virus, vers informatiques (*worms*), cheval de Troie et autres *malwares*, tels que les rançongiciels), ainsi que la falsification des supports papier.

Le matériel peut être espionné : il s'agit ici d'être observé ou écouté à l'intérieur ou à l'extérieur de locaux. Le matériel n'est pas endommagé, mais les informations peuvent être compromises : observation d'un écran, lecture indue de supports papier, écoute de conversations (réunions, discussions informelles, sur haut-parleurs, …), géolocalisation d'un matériel, interception des correspondances, reproduction de documents papier ou numériques (photocopie, photographie, etc.). À cette liste s'ajoutent les cas des *keylogger*, qui vont enregistrer la frappe des touches du clavier et les restituer, ainsi que d'autres logiciels espions (espiogiciels ou *spyware*), qui vont collecter des informations sur l'environnement au sein duquel il est installé, sur les usages habituels des utilisateurs du système, le tout, bien sûr, à l'insu du propriétaire et de l'utilisateur.

On retrouve donc ici, sans véritable surprise, la dualité entre l'aspect technique et l'aspect comportemental de la cybermalveillance et de la cybercriminalité, évoquée en introduction. Mais aussi utile soit-elle, cette opposition technique/comportemental n'est pas suffisante pour rendre compte de l'état des menaces pesant sur les cabinets.

49 - Voir par exemple la perte d'une clé USB contenant une copie des actes d'enquête sur les attentats terroristes de Charlie Hebdo et de l'Hyper Cacher, « *Charlie Hebdo. Une clé USB disparaît : grosse boulette des avocats* », Ouest France, 23 août 2016.

À côté des failles[50] de sécurité et des moyens techniques utilisés, il faut impérativement prendre la mesure des dangers résultant de ce que l'on appelle l'**ingénierie sociale (*social engineering*)**. Pour faire simple, dans ce dernier cadre, il n'est pas question de "pirater" directement les systèmes et réseaux, mais d'agir sur le comportement humain. La personne visée, considérée comme le « *maillon faible de la sécurité du système d'information* »[51], est manipulée, influencée (corruption, chantage, harcèlement, embrigadement, satisfaction de l'ego, etc.). L'idée est de l'amener à divulguer une information ou des données confidentielles ou à réaliser d'autres types d'actions (exécution d'un virement bancaire, communication d'un mot de passe, autorisation d'accès physique aux locaux, etc.). Les moyens malveillants sont alors introduits au sein de l'organisation en exploitant la confiance, l'ignorance ou la naïveté de la victime, par voie numérique ou non d'ailleurs (e-mail, téléphone, courrier, contact direct, réseaux sociaux, etc.).

La réalité montre que les "pirates" ont recours à différents procédés pour arriver à leurs fins, d'ordre non seulement technique, mais aussi organisationnel et personnel : ils couplent le plus souvent un procédé technique (un cheval de Troie, un rançongiciel, etc.), à l'exploitation d'autres informations, telles que des fichiers clients ou des organigrammes et annuaires permettant par exemple des usurpations d'identité (informations qui pourront être volées parce que mal sécurisées ou trop aisément accessibles en interne ou informations publiques, relayées par exemple sur le site internet du cabinet). On peut ici, sans trop de peine, imaginer le cas d'un hacker se faisant passer pour un avocat pour adresser un mail accompagné d'un fichier attaché piégé. Quel client ne l'ouvrirait pas ?[52]

« On peut sans peine imaginer l'usurpation de l'identité d'un avocat pour adresser des courriels accompagnés d'un fichier attaché piégé. Quel client ne l'ouvrirait pas ? ».

Outre les cas d'usurpation d'identité, la plupart des programmes développés dans le but de nuire à un système informatique ou au moyen de ce dernier, ne peuvent, concrètement, causer des dommages que grâce à l'action d'un utilisateur malintentionné ou insuffisamment sensibilisé aux risques. La plupart des *malware* (pour *malicious software*, logiciels malveillants) se déploient le plus souvent à partir d'une pièce jointe à un courriel ou de tout autre élément pouvant être téléchargé (photos, vidéos, musique, logiciels, appli, etc.), voire par un téléchargement inopiné lors de la consultation d'une page web ou d'une publicité malveillante. Un cas très répandu aujourd'hui[53] est le « *hameçonnage* » (ou *phishing*), qui vise à obtenir du destinataire d'un courriel frauduleux (mais d'apparence légitime), qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion ou bien encore qu'il mette à jour des données personnelles détenues par un tiers de confiance (services financiers, réseaux professionnels, administrations, etc.). Le plus souvent, en un clic, la victime est redirigée vers un site falsifié qui va recueillir l'ensemble des données saisies. Considéré comme la « *menace la plus sérieuse pour les organisations* »[54], un *ransomware* est un programme malveillant qui va empêcher l'accès aux données en les rendant illisibles. Souvent, il sera contenu dans une pièce jointe piégée (facture, bon de livraison, etc.) : à l'ouverture du document attaché, le logiciel s'installe et « *chiffre* » les données de la victime, puis peut s'étendre à tout le système d'information. Les données ne pourront alors être lues qu'avec une « *clé* » pour les décrypter, que seul le cybercriminel détient. Une rançon est demandée, souvent en crypto-monnaie (*Bitcoin*), en échange du mot de passe de déchiffrement.

La question ne semble donc pas tant être de savoir *si*, mais *quand* on va être attaqué. Loin de nous, une fois encore, l'idée de vouloir véhiculer uniquement un discours alarmiste. Il est tout à fait possible de gérer efficacement un incident cyber. En sus des mesures de cybersécurité, qui se concentrent, au sens strict, sur les solutions techniques de sécurité informatique permettant de réduire les risques, il faut être prêt à réagir lorsque le risque se réalisera. Et, pour limiter la portée de l'incident, il est important d'avoir préalablement déterminé les actions à réaliser et les comportements à adopter avant, pendant et après l'événement.

50 - Les failles sont des « *vulnérabilité[s] dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal* » (ANSSI, Glossaire, « Faille », www.ssi.gouv.fr).
51 - ANSSI, Glossaire, « Ingénierie sociale » (www.ssi.gouv.fr).
52 - Voir D. Bancal, « *Piratage d'avocats et de magistrats, une fuite de données sous la robe ?* », www.zataz.com, 14 sept. 2020.
53 - Une augmentation de 400 % des demandes d'assistance pour les faits de phishing a par exemple été constatée sur la plateforme Cybermalveillance.gouv.fr dès le début du confinement (J.-J. Latour, www.lesassisesdelacybersecurite.com).
54 - Voir not. Guide ANSSI-DACG, Attaques par rançongiciels, tous concernés, précité.

2.2. Se préparer à réagir à un incident cyber

En dépit d'une bonne sécurisation des équipements informatiques[55] et d'une sensibilisation efficace et régulière des utilisateurs[56], le risque d'une cyberattaque ne peut pas être complètement écarté. Et, « *en matière de protection des systèmes d'information, l'anticipation est la clé* »[57]. Il faut donc bâtir une véritable politique de sécurité, adaptées aux spécificités du cabinet. Et c'est ici que l'accompagnement par un spécialiste prendra particulièrement tout son sens (réalisation d'audits, construction d'un plan de gestion de crise, gestion de la crise cyber en temps réel), sans d'ailleurs que cela implique forcément un budget démesuré. Dans un monde idéal, toutes les organisations disposeraient de moyens et de ressources dédiées, auraient un plan de gestion de crise et de pouvoir s'appuyer sur une équipe interne qualifiée. Il est certain que la réalité est toute autre…

Un premier défi pour le non-spécialiste est de savoir réagir dans l'urgence, pour limiter les impacts d'une attaque. En effet, si, en dépit des précautions prises, une cyberattaque survient, il faut avoir à l'esprit qu'une mauvaise réaction peut avoir pour conséquence, sinon d'aggraver la situation, du moins d'empêcher le traitement efficient du problème. En raison de la diversité des cybermalveillances, il serait inopportun – pour ne pas dire contreproductif – d'envisager une seule bonne manière de réagir à une cyberattaque. Il n'existe pas de solution universelle ; tout dépendra notamment de la nature de l'événement et de son ampleur. Évidemment, nous laissons (bien volontiers !) les experts en la matière déployer leur savoir-faire. Mais la connaissance de quelques principes de base peut permettre au cabinet d'agir rapidement pour « *limiter les dégâts* ». Une description succincte et toutes proportions gardées, de ce qu'il est préconisé de faire peut s'avérer salutaire.

Il est certain que pour pouvoir réagir à une cyberattaque, encore faut-il avoir pu la détecter… sachant que plus l'attaque s'étire dans le temps, plus elle sera complexe à gérer. **La détection est donc le point de départ de la gestion de l'incident.** Le constat d'un comportement inhabituel d'un poste de travail est ici, sans surprise, un bon indicateur : ordinateur fortement ralenti, connexion impossible, problème de droits d'accès à une application métier, alertes de l'anti-virus, modifications non volontaires de fichiers ou de la page d'accueil du site du cabinet, fonctionnalités activées sans autorisation, multiples alertes de l'antivirus, publicités intempestives abondantes, perte de l'espace de stockage sur les serveurs, arrêt intempestif du poste de travail, etc. D'où l'importance d'utiliser *a minima* un antivirus et un pare-feu (*firewall*) et de maintenir à jour ces éléments, ainsi, d'ailleurs, que les applications et logiciels métiers utilisés[58]. Les choses pourront être assez imperceptibles, par exemple si l'auteur de l'attaque dispose de beaucoup de temps : il agira par "petites touches", difficilement détectables, mais qui, mises "bout à bout", finiront par provoquer d'importants dégâts. À l'inverse, l'attaque pourra être très évidente, notamment si le cabinet est victime d'un type de cyberattaque particulièrement en vogue, par rançongiciel. Une demande de rançon pour pouvoir récupérer les données chiffrées s'affichera à l'écran, éventuellement avec un décompte de temps avant leur destruction ou leur divulgation.

Dans ce cas spécifique d'une attaque *ransomware*, **ne pas payer la rançon** ! Pour le reste, il faut exécuter les **gestes de « premier secours »**, tout en gardant son calme… Le **premier réflexe est de déconnecter l'ordinateur du réseau, mais non de l'éteindre.** En débranchant le câble de connexion à internet ou en désactivant la connexion wifi, toutes les communications vers et depuis Internet seront bloquées. Cela permettra non seulement de stopper l'attaque et de réduire les risques de fuite de données, mais aussi de limiter sa propagation à d'autres

55 - Ainsi que leur maintien en condition de sécurité (MCS).
56 - Sur la mise en place de bonnes pratiques d'hygiène numérique, voir *infra*, § 4.
57 - Guide ANSSI-CCA, Organiser un exercice de gestion de crise cyber, oct. 2020 (www.ssi.gouv.fr).
58 - Sur ce point, voir les recommandations de bonnes pratiques *infra*.

appareils que celui qui est ainsi isolé. En revanche, il ne faut pas éteindre l'ordinateur, ni le redémarrer. Ce faisant, le risque est en effet de perdre des informations utiles pour l'analyse de l'attaque, en supprimant toute possibilité de remonter à l'auteur de l'attaque (préservation des preuves). Il n'est pas recommandé de procéder à une sauvegarde des données à ce moment-là, au risque d'amplifier le phénomène et de contaminer les supports de stockage amovibles (clés USB, disque dur externe, cartes mémoires, etc. ; d'où l'importance, une fois encore, de faire en amont et régulièrement des sauvegardes…).

Le **deuxième réflexe est de commencer à documenter l'évènement**, en retraçant les faits liés à l'incident : date et heure, nom de la personne à l'origine de l'action ou ayant été informée de l'évènement, description factuelle de ce qui s'est passé. L'idée est de pouvoir retrouver les circonstances dans lesquelles les données et outils ont évolué : traçabilité des actions menées, authentification des utilisateurs, imputabilité du responsable de l'action effectuée. Ce « *journal* » sera progressivement complété pour expliciter les actions réalisées au cours des périodes entourant la survenance de l'incident. Cela pourra également faciliter les investigations numériques (*digital forensic*) qui seraient menées par la suite.

Le **troisième réflexe est d'avertir** (la hiérarchie, ses confrères, les membres du cabinet) **et de trouver une assistance technique** : auprès du référent en sécurité des systèmes d'information du cabinet, auprès du prestataire spécialisé en cybersécurité au titre du contrat conclu avec le cabinet ou bien encore par l'intermédiaire de la plateforme *cybermalveillance.gouv.fr* mise en place pour le gouvernement pour aider les entités ne disposant ni des ressources, ni de l'expertise nécessaire. La plateforme permet, après un diagnostic personnalisé, d'être mis en relation avec un réseau de professionnels en sécurité numérique de proximité. Une réaction rapide est essentielle à la maîtrise de l'incident. Mais pour échanger, il peut être prudent de ne plus utiliser les systèmes et réseaux habituels, qui peuvent avoir été compromis, et d'utiliser des outils alternatifs.

Concomitamment, il faut **diagnostiquer l'incident, le traiter** et **évaluer la gravité des événements.** Cela suppose la plupart du temps l'aide d'un spécialiste, voire l'activation d'une cellule de crise, si le fonctionnement du cabinet était fortement impacté par l'attaque. Leur tâche sera de définir et de piloter les actions nécessaires pour enrayer l'incident, sécuriser l'environnement informatique et sortir de la crise. En somme, d'organiser la réponse adéquate sur les plans à la fois technique, organisationnel et opérationnel. C'est ainsi que l'on mesure l'intérêt de l'élaboration, en amont, d'une politique de management du risque cyber, « *pour endiguer les effets de la crise d'une part, et rétablir le bon fonctionnement des systèmes d'autre part* »[59]. Prendra en effet tout son sens, le fait de disposer de **plans de continuité et de reprise d'activités** et d'une stratégie de communication spécialement établis en vue de la gestion d'une crise cyber. L'ensemble de ces mesures suppose une organisation spécifique, qui pourra être préparée lors d'audits en cybersécurité. Ceux-ci permettront à la fois d'évaluer les risques, de construire des scénarios stratégiques et opérationnels et de prévoir le traitement des incidents cyber. Le plan de continuité d'activités (PCA) a pour vocation d'organiser la poursuite des activités dans les meilleures conditions possibles. Le but est de pouvoir continuer à travailler, même de manière dégradée : continuer à être joignable par les clients, à gérer les actes de procédure, etc. Il pourra par exemple s'agir de disposer d'un ordinateur portable pouvant être utilisé en remplacement du poste fixe ou d'une technologie internet de secours (connexion satellite, clé 4G). Avoir une vision exacte des dossiers pour lesquels le dépôt au greffe des actes en version papier sera envisageable (avec une argumentation prête pour invoquer la cause étrangère…) et de ceux dans lesquels il faudra demander un renvoi entre également dans la préparation. Avec un plan de continuité d'activités préparé à l'avance, le cabinet reste opérationnel pour répondre aux attentes et besoin de ses clients, même si ce n'est pas dans les conditions habituelles. La mise en œuvre d'un plan de reprise d'activités (PRA) sera lui, le cas échéant, nécessaire pour remettre le système d'aplomb et retrouver l'usage des équipements informatiques qui auraient été rendus inutilisables et de restaurer, autant que possible, les données affectées, ce qui peut prendre du temps. Il s'agira aussi d'apporter les correctifs nécessaires, notamment sur un

59 - G. Poupard, Édito, Guide ANSSI-CCA, Organiser un exercice de gestion de crise cyber, précité.

plan technique, pour éviter que l'incident ne se reproduise.

« Avec un plan de continuité d'activités préparé à l'avance, le cabinet reste opérationnel pour répondre aux attentes et besoin des clients, même si ce n'est pas dans les conditions habituelles ».

Le **contrôle de la communication, interne et externe**, sera également essentiel. Il faut en effet non seulement organiser les échanges avec les personnes en charge de la gestion technique de l'incident et les associés du cabinet, mais aussi prévenir les autres membres du cabinet : leur communiquer les actions à réaliser à leur niveau, leur indiquer les personnes à qui s'adresser pour faire remonter les informations, les tenir régulièrement informés de l'évolution de la situation. Au besoin, il pourra être utile de rappeler la mise en œuvre de la clause de confidentialité pour maîtriser les échanges, particulièrement à l'égard des médias et sur les réseaux sociaux. **D'autres actions « *de communication* », quasi-intuitives chez les professionnels du droit, seront aussi à réaliser à bref délai :** notifier la violation de données personnelles à la CNIL, prendre contact avec les autorités policières pour envisager un dépôt de plainte et, le cas échéant, solliciter son assureur, particulièrement si le cabinet a souscrit à une couverture en cybersécurité (mais pas seulement : la RCP pourrait couvrir un dépassement de délai occasionné par l'impossible dépôt par voie électronique et les conséquences liées aux sanctions procédurales en découlant). Il faudra aussi, une fois que l'incident sera globalement maîtrisé et en fonction des conséquences de ce dernier, songer à informer les clients et les partenaires du cabinet. Le cas échéant, il pourra également être opportun de penser à prévenir l'Ordre, ne serait-ce que pour qu'une communication soit adressée à l'ensemble des confrères du Barreau, aux fins de les inviter à une vigilance renforcée.

À la fois en termes de prévention et de réponse aux attaques, « *plus les choses auront été préparées en amont, notamment la cartographie des risques, l'analyse des vulnérabilités et des vecteurs et modes d'attaques, plus la gestion de la crise pourra être efficiente* »[60]. **Savoir quoi faire et à qui s'adresser, à quel moment et par quel biais ou bien encore se pré-constituer des réponses pour gérer sa communication seront indispensables pour affronter un incident cyber,** surtout s'il est d'une particulière gravité. Mais même si la gravité est moindre, avoir une bonne perception de la conduite à tenir supposera d'avoir, en amont, étudié les événements redoutés, apprécié les risques, préparé des scénarios de menaces et planifié la réponse. Pouvoir accéder rapidement à des documents aide-mémoire (réflexes, actions à réaliser, fiches contact, etc.) sera utile, tout comme le fait de pouvoir compter sur des collègues non seulement sensibilisés, mais aussi exercés. D'ailleurs, outre la réalisation d'une analyse des risques complète, bon nombre de consultants en cybersécurité proposent la réalisation de simulations permettant à chaque membre du cabinet de s'exercer à agir et réagir de manière adéquate. « *Face à une menace informatique toujours croissante et en mutation, l'amélioration de la résilience numérique par l'entraînement à la gestion de crise cyber n'est plus seulement une opportunité, mais bien une nécessité pour toutes les organisations* »[61].

« Plus les choses auront été préparées en amont (…) plus la gestion de la crise pourra être efficiente ».

On l'aura compris, faire un inventaire précis des données et informations dont dispose le cabinet, s'informer sur les cybermalveillances, faire réaliser une analyse des risques et disposer d'un accompagnement par un spécialiste tendent à devenir un « *passage obligé* » pour assurer la sûreté numérique du cabinet. Ne serait-ce que pour pouvoir affronter et surmonter la crise, bien que les avantages de la mise en place des mesures à la fois préventives et réactives pour gérer les risques auxquels le cabinet est exposé ne se mesurent pas qu'en termes techniques et opérationnels. La démarche a vocation à s'inscrire dans la durée, selon une logique continue d'amélioration et d'ajustement. **Mais intégrer dès à présent la gouvernance du risque numérique dans le fonctionnement quotidien de sa structure d'exercice est une démarche qui s'avèrera, avec certitude, « *payante* » à plus ou moins long terme.** C'est pourquoi l'avocat doit valoriser son engagement et les investissements qu'il réalise en la matière.

60 - INHESJ, juill. 2015, Comment organiser une cellule de crise en cas de cyberattaque ?, Travaux des auditeurs (www.cigref.fr).
61 - G. Poupard, Édito, Guide ANSSI-CCA, Organiser un exercice de gestion de crise cyber, oct. 2020 (www.ssi.gouv.fr).

Partie 3. Évaluer et réduire le risque cyber : quels intérêts pour l'avocat ?

Comme pour les autres organisations, « *une cyberattaque peut rapidement mettre en péril la survie de l'organisation qui la subit ou, sans aller jusque-là, nuire gravement et durablement à son image et à la confiance qu'on lui accorde* »[62]. Engagement de la responsabilité, atteinte à l'image, altération de la confiance des clients et partenaires de travail et pertes financières font partie des conséquences d'un incident cyber qu'il est essentiel de mesurer. Outre la limitation de ces impacts, essentielle pour la pérennité même du cabinet, se mobiliser pour assurer la sûreté numérique a une résonance particulière au regard des valeurs et obligations de la profession.

3.1. Mesurer les impacts d'un incident cyber au bénéfice de la pérennité du cabinet

La détermination des impacts d'un incident cyber fait partie de l'analyse qu'un *risk manager* (expert interne ou partenaire spécialisé) sera en mesure de réaliser. Il fera le lien entre ce que peut raisonnablement craindre le cabinet et ce à quoi il est réellement exposé. Les événements redoutés (fuite de données, altération d'un fichier, usurpation d'identité, espionnage, etc.) seront étudiés avec précision et mis en scène, de manière réaliste, par rapport à l'activité du cabinet et aux valeurs de la profession. La construction de ces scénarios permettra également d'évaluer la vraisemblance de la survenance des incidents, de les catégoriser selon une échelle de gravité propre à chaque structure d'exercice et de proposer la mise en place de mesures propres à réduire les risques à un niveau acceptable. « *Le coût de la prévention, en faisant appel à des experts sera toujours moins important que le coût de la nécessité de réparer une fuite de données* »[63].

Les conséquences d'un incident cyber sont de plusieurs natures et peuvent revêtir différents niveaux de gravité. Elles peuvent aussi, sans surprise, se cumuler au détriment tant du cabinet, que de son/ses client(s). Plus précisément, on y trouve des **impacts sur le fonctionnement**. Ceux-ci se mesurent, comme déjà évoqué, sur la capacité à réaliser les missions et fournir la prestation attendue. Un incident cyber peut également altérer les capacités de décision, avec une perte de la marge de manœuvres. Des **impacts humains** peuvent également résulter d'un incident cyber, avec des conséquences directes ou indirectes sur l'intégrité physique des personnes (menaces de l'avocat lui-même ou de ses proches, mise en danger d'une personne bénéficiant de l'anonymisation de son témoignage, etc.) et sur le lien social interne (perte de confiance des collaborateurs et salariés, exacerbation de tensions, pression médiatique…). Évidemment, s'agissant des avocats, surviendront vraisemblablement des **impacts sur le patrimoine informationnel** : perte de données, de savoir-faire et des capacités d'innovation, à la fois du cabinet lui-même (qui aurait créé une *legaltech* par exemple) et du client, dont les activités et les données pourraient être mises en péril. Des **impacts financiers** seront aussi très probablement subis par le cabinet : perte de chiffre d'affaires (particulièrement en cas de clause d'honoraires de résultat, mais aussi en cas de faux ordre de virement), dépenses imprévues liée au rachat d'équipements informatiques, à la restauration des données, aux frais d'expertise (*digital forensic*), à la perte d'un appel d'offre (en raison d'un niveau

62 - ANSSI-AMRAE, Maîtrise du risque numérique. L'atout confiance, édito du Guide (www.ssi.gouv.fr).
63 - S. Vara, Présidente de la Commission numérique du Conseil National des Barreaux, lors des e-débats du CNB du 25 juin 2020. Voir « *Cybersécurité des cabinets d'avocats : il est urgent et assez simple de s'en préoccuper* » (www.village-justice.com.)

de cybersécurité insuffisant par exemple[64]) et à d'autres "pénalités" (indemnisation du client pour perte de chance, en cas de faute de l'avocat, sanctions administratives/pénales en cas de non-conformité au RGPD, etc.). **L'impact sur la réputation** et l'image de marque, sur la notoriété et la renommée pourra être assez dévastateur, entraînant une perte de crédibilité vis-à-vis des clients, d'une position concurrentielle du cabinet, etc. Atteinte à la réputation et au renom qui, selon son retentissement médiatique et sur les réseaux sociaux, serait plus ou moins indélébile. Le cas échéant, cela pourrait d'ailleurs impliquer la mise en œuvre de voies de droit pour mettre un terme à l'atteinte à la réputation constatée.

« Les effets d'une atteinte à la confidentialité, à la disponibilité ou à l'intégrité des données et informations détenues par un cabinet d'avocat se déploient bien au-delà de leur impact opérationnel ».

D'autres effets préjudiciables des incidents cyber vont être décuplés en raison des missions de l'avocat et de l'étendue de sa responsabilité professionnelle au titre des devoirs et obligations déontologiques de la profession. On pense ici évidemment à **l'impact juridique**, lié à l'engagement potentiel de la responsabilité de l'avocat (faute civile, déontologique, pénale) **et ce qui s'en suivra en termes financiers et réputationnels**. Tel sera particulièrement le cas dans l'hypothèse d'une fuite de données sensibles rendues possibles par un comportement négligent ou par l'exploitation d'une faille dans la sécurité informatique. Les effets pourraient être considérablement démultipliés — et la responsabilité du cabinet corrélativement engagée — si l'attaque venait à se propager à partir du cabinet vers les systèmes d'information des clients. La diffusion non contrôlée (éventuellement simplement prématurée) de certaines informations, telles que l'état de cessation des paiements d'un client, l'intention d'engager une action en justice, un projet de fusion-acquisition, la préparation d'un plan social, etc. Cette révélation serait susceptible d'impliquer une perte de la maîtrise du projet du client ou d'une capacité de négociation, par exemple dans le cadre d'un règlement alternatif du différent. L'incident pourra aussi imposer une adaptation des stratégies d'accompagnement du client, avec une éventuelle surcharge de travail, sans compter, ici encore, l'impact financier (selon les termes de la convention d'honoraires conclue), le possible engagement de la responsabilité du praticien et les conséquences sur son image. Le tout, avec des niveaux de gravité variables selon les circonstances propres à l'affaire, au client et au cabinet.

Prenons un autre exemple, celui d'un incident cyber rendant impossible l'accès au système d'information, l'usage des équipements informatiques et/ou l'indisponibilité prolongée de la messagerie électronique. S'il s'agit d'un *ransomware* et que toutes les données seraient indisponibles en raison du chiffrement et qu'aucune sauvegarde des données n'était disponible, l'activité pourrait être durablement affectée. Même avec un incident de moindre gravité, l'évènement aurait forcément un impact sur le fonctionnement du cabinet, ne serait-ce que par la nécessité de l'utilisation de moyens de communication alternatifs. Empêchant l'accès aux fichiers et données des dossiers en cours, voire au RPVA, il rendrait impossible, à bref délai, la rédaction d'un acte de procédure et/ou sa remise électronique dans les temps et obligerait, le cas échéant, à déposer le support papier au greffe, dans ses horaires d'ouverture... Pour beaucoup de procédures, il en découlera donc un risque accru de caducité ou d'irrecevabilité de la demande. Outre ces sanctions procédurales, la responsabilité civile professionnelle de l'avocat pourrait être recherchée pour défaut de diligences, quand bien même la cause étrangère aurait vocation à être invoquée ici[65].

Nul besoin de multiplier davantage les exemples pour comprendre que les conséquences d'un cyber incident peuvent être pour le moins fâcheuses, voire désastreuses. Chacun de ces impacts internes, externes, directs et indirects doivent donc être identifiés et évalués en termes de gravité. De la même manière que l'analyse d'impact relative à la protection des données (AIPD) constitue un « *outil important de responsabilisation et de conformité qui permet de garantir le respect des principes du RGPD de façon opérationnelle et de pouvoir le démontrer* »[66],

64 - Un diagnostic de cybersécurité satisfaisant en fonction des enjeux du marché public pourrait prochainement devenir l'un des critères de choix (voir la proposition de loi pour la mise en place d'une certification de cybersécurité des plateformes numériques destinées au grand public, Sénat, PP n° 629-19/20, 15 juill. 2020).

65 - Voir not. CA Paris, 12 févr. 2020, RG n° 19/17629 ; CA Nîmes, 28 juill. 2020, RG n° 19/04433.

66 - CNIL, Ce qu'il faut savoir sur l'analyse d'impact relative à la protection de données (www.cnil.fr).

l'analyse des risques cyber pourrait bien avoir vocation à devenir un outil indispensable à la gestion des structures d'exercice, de surcroît s'agissant d'une profession soumise à un devoir de confidentialité et à un secret professionnel renforcés. Ne pas se soucier d'assurer suffisamment la sûreté numérique s'avère être un pari plus que risqué au regard des valeurs et obligations mêmes de la profession.

3.2. Se mobiliser pour la sûreté numérique au regard des valeurs et obligations de la profession

Mettre la sûreté numérique en perspective des valeurs et obligations de la profession d'avocat permet de raisonner en replaçant le praticien au sein de son écosystème. **Cette approche conduit à se demander quelles garanties l'avocat offre à son client, en termes de sécurité numérique, pour construire ou nourrir la relation de confiance indissociable de l'exercice de la profession.** Elle renvoie ainsi aux principes essentiels de la profession, particulièrement en termes de prudence, de confidentialité et de secret professionnel. L'état d'insécurité numérique résultant d'une protection insuffisante du cabinet incite en effet à s'interroger sur la responsabilité de l'avocat, à raison notamment des dommages qu'un cyber incident subi par le cabinet pourrait causer à ses membres et/ou aux tiers. En revanche, la construction d'une solide sûreté numérique du cabinet, associée à ces principes déontologiques qu'elle permettrait de consolider, pourrait permettre à l'avocat de se placer dans une situation privilégiée sur le marché de la prestation juridique.

Au niveau européen, comme au niveau national, les dispositions relatives aux principes essentiels de la profession évoquent le secret professionnel de l'avocat et la confidentialité de ses échanges et correspondances essentiellement sous l'angle d'une obligation déontologique pour le praticien et d'un droit fondamental du client. De son côté, la Cour européenne des droits de l'homme considère de longue date que le secret professionnel est la base de la relation de confiance entre l'avocat, tant au nom du droit à la vie privée, que sur le fondement du droit à un procès équitable. Et ces principes sont évoqués pour sanctionner les ingérences injustifiées, émanant notamment des autorités étatiques. Les échanges entre un avocat et son client, quelle qu'en soit la forme, doivent être hors de portée d'ouïe et de la lecture par les tiers. **Il est certain qu'un avocat ne peut mener à bien sa mission fondamentale, s'il n'est pas à même de garantir à ceux dont il assure la défense ou le conseil, que leurs échanges demeureront confidentiels, y compris dans l'espace numérique.**

> ***« L'avocat ne peut mener à bien sa mission fondamentale, s'il n'est pas à même de garantir à ceux dont il assure la défense ou le conseil, que leurs échanges demeureront confidentiels, y compris dans l'espace numérique ».***

Avec la digitalisation, « *le monde judiciaire change. Les contours du secret professionnel aussi* »[67] ; le monde numérique change, les contours de la confidentialité aussi. Or la plupart des règles ont été établies pour des documents papier et des discussions orales. Elles tendent, progressivement, à se déployer dans l'espace numérique avec l'encadrement de l'interception des correspondances, des perquisitions et saisies informatiques, du recours à l'IMSI-catcher et autres techniques spéciales d'enquête permises notamment dans le cadre de l'enquête en criminalité organisée. La confidentialité numérique y est conçue comme une obligation imposée à l'État, de respecter le secret, par exemple des correspondances émises par la voie des communications électroniques[68]. Mais avec des difficultés en ce qui concerne la protection des cabinets d'avocat, qui ont pu être soulignées à propos de l'accès aux données de connexion, accentuées par l'absence de disposition constitutionnelle consacrant le droit au secret des échanges et correspondances des avocats[69].

Qu'en est-il du côté du client de l'avocat ? Les obligations imposées aux avocats eux-mêmes, en matière de sécurité informatique ne sont, pour l'instant du moins, exprimées qu'en termes de recommandations générales, sauf à s'inscrire dans le cadre précis de la protection des données personnelles au sens du RGPD. Cependant, le Code de déontologie des avocats européens prévoit que « *les avocats doivent maintenir et développer leurs connaissances et leurs compétences professionnelles en tenant compte de la dimension européenne de leur profession* »[70].

67 - D. Soulez Larivière, Le secret professionnel et l'éthique de l'avocat, Dalloz Avocats n° 11, nov. 2018, p. 374.
68 - CSI, art. L. 241-1.
69 - Cons. const., 24 juill. 2015, n° 2015-478 QPC, JO 26 juill. (Association French Data Network et autres).
70 - Code de déontologie de l'avocat européen, art. 5.8.

Et le Conseil des Barreaux européens en déduit explicitement que « ***de ces exigences découle un impératif de plus en plus présent pour les avocats d'acquérir les compétences pouvant s'avérer nécessaires pour garantir la protection des informations confidentielles des clients dans le monde virtuel*** »[71]. Certains estiment d'ailleurs qu'« *il est regrettable que le règlement intérieur national n'intègre pas, parmi les obligations déontologiques de l'avocat, cette nécessité pour les avocats de protéger le secret professionnel de toutes les atteintes liées aux nouvelles technologies* »[72].

Au-delà du seul cadre du RGPD et peut-être sans aller jusqu'à reconnaître la nécessité de consacrer un « *devoir de l'avocat d'être technologiquement compétent* »[73], il n'en reste pas moins presque certain qu'**assurer la sûreté numérique du cabinet est, concrètement, le moyen de rendre plus effective l'obligation de confidentialité prévue à l'article 3 du Règlement Intérieur National** (RIN). Or, dans ce cadre de l'engagement de la responsabilité de l'avocat, il faut bien tenir compte de l'état incertain de la jurisprudence, qui pourrait bien finir par considérer qu'un cyber incident ne répond pas aux conditions d'imprévisibilité et d'irrésistibilité de la force majeure, au sens de l'article 1218 du Code civil[74].

« Une obligation de moyens pourrait bien finir par émerger et devenir opposable à l'avocat en matière de cybersécurité ».

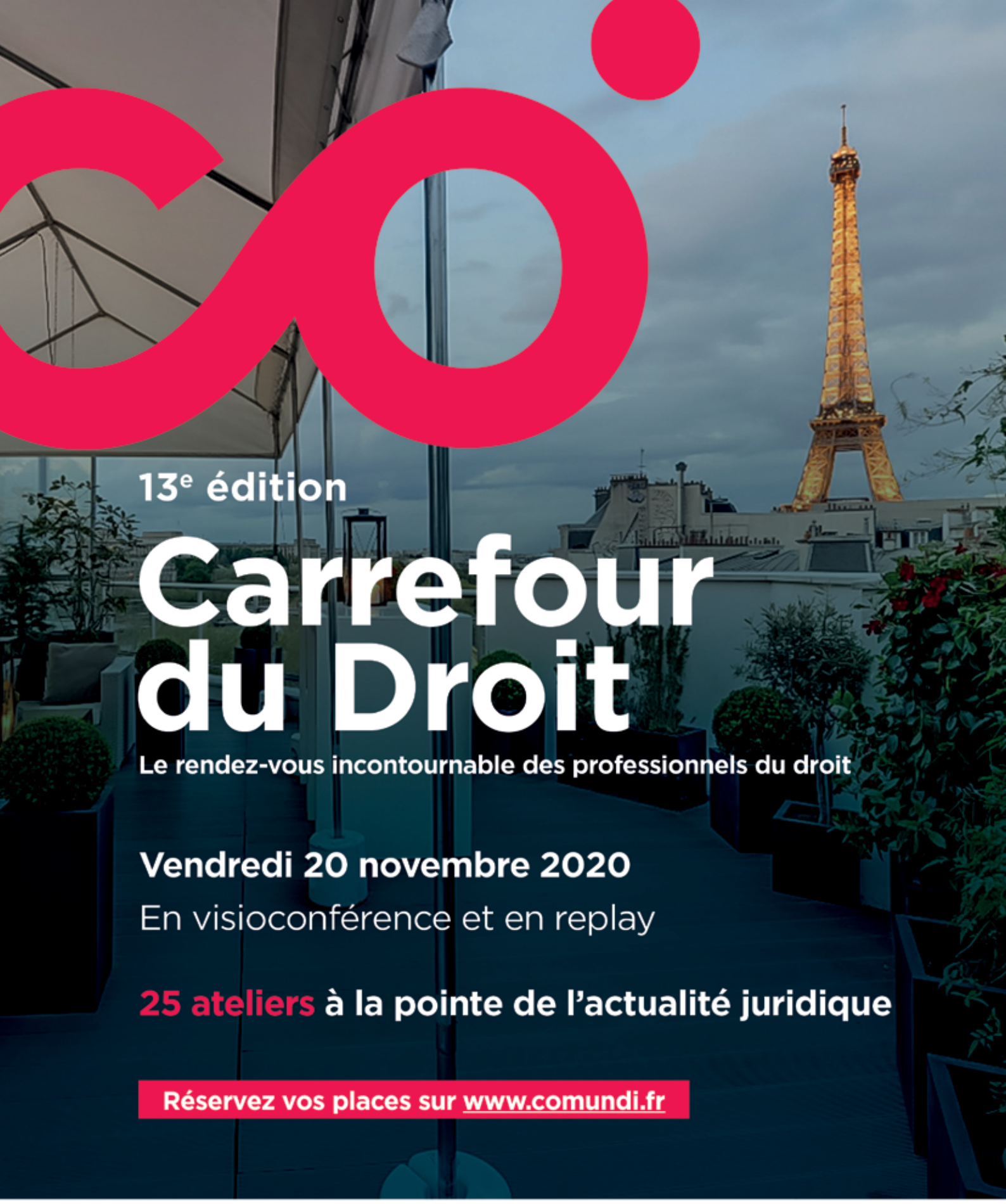
Sans aller jusqu'à envisager une obligation de résultat, une obligation de moyens pourrait donc bien finir par émerger et devenir opposable au praticien en matière de cybersécurité. Et cette obligation aurait une portée d'autant plus large que l'avocat doit faire respecter le secret non seulement par les membres du personnel de son cabinet, mais aussi, sauf disposition contractuelle particulière, « *par toute personne qui coopère avec lui dans son activité professionnelle* ». Or il faut avoir à l'esprit que la fuite de données pourrait aussi résulter des conditions de travail d'un prestataire extérieur, auquel il est fait appel pour externaliser la réalisation de certaines tâches du cabinet : standard téléphonique et secrétariat à distance, traducteur, *cloud computing*, gestion du site web, sites de référencement, de consultation en ligne, etc., sans oublier la gestion de la sécurité informatique elle-même.

Quels seraient alors les moyens dont disposerait l'avocat pour se protéger contre des poursuites pour manquement à la déontologie ou, plus largement à la sécurisation des données et informations confiées ou créées par le cabinet ? La solution n'est évidemment pas inconnue des professionnels du droit ; elle consiste dans un transfert des risques.

Une première hypothèse est celle de l'externalisation informatique, qui permettra à la fois de doter le cabinet d'une architecture sécurisée et de transférer le risque cyber. Le prestataire est tenu de prendre des mesures pour assurer la sécurité des données, quelle que soit la forme de la prestation (*data center, cloud computing*[75]). Un prestataire a ainsi pu être condamné à indemniser son client en raison de l'absence de sauvegarde des données par le logiciel en cause, en raison d'une anomalie dans l'écriture des programmes imputable au fournisseur[76]. Mais comment reporter sur lui l'obligation de confidentialité renforcée des données gérées par le cabinet ? Il sera essentiel non seulement d'évaluer les risques de l'infogérance en ce qui concerne la divulgation des données (compétence du prestataire ? nationalité ? lieu d'hébergement des données ? sécurité de l'infrastructure et réalisation d'audits réguliers ? absence de sous-traitance ? etc.) et de prendre un soin tout particulier dans la rédaction d'une solide clause de confidentialité au sein du contrat d'infogérance (comme d'ailleurs d'une clause de réversibilité pour pouvoir récupérer les données lorsqu'il sera mis fin à l'exécution du contrat). Et ces précautions valent d'ailleurs pour tout type de tâches externalisées. Comme le rappelait le CCBE en prônant la création d'un impératif déontologique, « *même si l'avocat choisit de déléguer ou de sous-traiter auprès d'experts techniques la prise de mesures spécifiques pour assurer la sécurité informatique en général ou la confidentialité en particulier, un niveau minimum de connaissances et de compétences doit encore entrer dans la gestion des cabinets d'avocats. Dans le cas contraire, les avocats du cabinet seront personnellement responsables de l'absence de contrôles de sécurité informatique, tout comme ils le seraient en cas d'absence de contrôles internes pour la gestion des fonds ou des documents des clients* »[77].

Mais même avec toutes ces précautions, le risque cyber ne pourra pas être réduit

71 - CCBE, 2016, Conseils pour le renforcement de la sécurité informatique des avocats contre la surveillance illégale (www.ccbe.eu).
72 - M. Bénichou, Le secret professionnel soumis aux technologies nouvelles, Dalloz Avocats n° 11, nov. 2018, p. 378.
73 - J. Gurtner, Les nouvelles technologies et la responsabilité des avocats : la cybersécurité et l'intelligence artificielle, in C. Chappuis, B. Winiger (dir.), Responsabilité civile et nouvelles technologies, Journée de la responsabilité civile 2018, Univ. Genève, Schulthess éd. romandes, 2019, p. 45 et s.
74 - Voir par ex. CA Paris, 7 févr. 2020, RG n° 18/03616, *cit. in* C. Théard-Jallu, K. Ishac, « *Victimes de ransomware : vous êtes potentiellement responsables, vérifiez vos contrats et surtout, ne payez pas !* », 16 oct. 2020 (www.degaullefleurance.com).
75 - Location de l'infrastructure informatique (IaaS, *Infrastructure as a Service*), plateforme avec gestion de ses propres applications (PaaS, *Platform as a Service*) ou offre de fonctionnalités par un logiciel (SaaS, *Software as a Service*).
76 - Cass. com., 11 déc. 2007, n° 04-20,782.
77 - CCBE, Conseils pour le renforcement de la sécurité informatique des avocats, précité.



13e édition

Carrefour du Droit

Le rendez-vous incontournable des professionnels du droit

Vendredi 20 novembre 2020

En visioconférence et en replay

25 ateliers à la pointe de l'actualité juridique

Réservez vos places sur www.comundi.fr

Legal & Network
La nouvelle marque juridique qui monte !

En partenariat avec :
LexisNexis®

comundi
compétences

à zéro et c'est vers le système assurantiel qu'il est donc opportun de se tourner. Au regard des critères d'assurabilité des risques[78], la question de l'assurance cyber est complexe[79] : « *les modèles d'assurance doivent être croisés avec la cartographie du risque cyber. Or, ce risque est mouvant et les dommages ne sont pas nécessairement physiques donc difficilement chiffrables* »[80]. Il existe pourtant une offre assurantielle qui s'étoffe progressivement, mais avec des modalités et des niveaux de couverture extrêmement variables d'un contrat à un autre, tant en ce qui concerne la quantification du risque, que la définition de la prime d'assurance. Perte de données et fraudes, intentionnelles ou par maladresse, gestion de crise, frais de notification et prise en charge du manquement à l'obligation de notification, mesure d'urgence et gestion de crise, restauration de données et investigations numériques (*forensic*), atteinte à la réputation, pertes d'exploitation… Tous les impacts d'un cyber incident sont susceptibles d'entrer dans le champ de la couverture. Certains seront déjà inclus dans le contrat de responsabilité civile professionnelle (responsabilité en cas de violation de données à caractère personnel, inexécution contractuelle en raison de l'impact de fonctionnement de l'incident).

Il faut donc commencer par auditer les contrats d'assurance déjà souscrits par le cabinet. Il est en effet tout à fait possible que le risque numérique soit déjà couvert, au moins partiellement, même si la tendance est davantage à une exclusion du risque numérique, au profit de polices d'assurance plus spécifiques. Il pourra également être utile de s'informer auprès de l'Ordre pour savoir si une couverture collective a été souscrite en faveur des praticiens inscrits au Barreau. Si le cabinet n'est pas encore couvert à ce titre ou si la couverture s'avère insuffisante au regard des risques auxquels le cabinet est exposé (évalués de manière réaliste, notamment à l'issue d'un audit cyber approfondi…), il faudra se lancer dans la quête d'une assurance adaptée, en sollicitant, au besoin les services d'un courtier. Mais il faut aussi avoir à l'esprit que des prérequis d'éligibilité peuvent être demandés par la compagnie d'assurance, tels que l'utilisation de logiciels antivirus et de pare-feu sur l'ensemble des appareils informatiques, serveurs et réseaux entre autres, la réalisation d'une sauvegarde régulière des données, l'absence de perte ou de vol de données dans les mois/années précédents, la sensibilisation des collaborateurs, etc.

Quel que soit le cas de figure, il s'avère que l'avocat est, peu ou prou, tenu de démontrer que des mesures suffisantes de précaution et de protection du système d'information et des données ont été mises en place. Le temps serait-il venu, avec la démultiplication des échanges dématérialisés et l'ampleur croissante des cyber incidents, de consacrer aussi une nouvelle facette des devoirs de l'avocat, énoncé de manière générale à l'article 1.3 du RIN, celui de « *faire preuve, à l'égard de ses clients, de compétence, de dévouement, de diligence et de prudence* » ? Au-delà donc, s'agissant de la prudence, de son cantonnement, en 2011, à l'opération juridique pour laquelle le concours du praticien est sollicité[81] ?

« *C'est par ce souci constant du respect de leurs obligations déontologiques dans l'univers du numérique que les avocats peuvent espérer réussir cette évolution inéluctable qui accompagne le développement de leur cabinet, sans perdre leur valeur et la confiance de leurs clients, en s'assurant en premier lieu de la sécurité des données du cabinet et du respect du secret professionnel* »[82]. **En présence de clients, personnes physiques ou morales, de plus en plus soucieux de la protection de leurs données, la cybersécurité du cabinet contribuera indéniablement à renforcer la position de l'avocat en tant que partenaire de confiance.** Rassurer ses clients et partenaires quant à la gestion sécurisée de leurs données ne peut ici être que bénéfique. Il ne faut pas hésiter à proposer (voire insister !) aux clients d'utiliser des modes de communication qui permettront le chiffrement des données échangées. **Travailler dans un environnement sécurisé conduit à s'engager dans un cercle vertueux, bâti sur une nouvelle forme d'affirmation du professionnalisme du praticien.** Dans le prolongement de ce crédit de confiance déterminant de la relation-client, les bénéfices de bonnes pratiques se mesurent en termes concurrentiels[83]. Dans une démarche de *business development* sur le marché de la prestation juridique, la sûreté numérique du cabinet pourrait bien, en effet, être une manière de convaincre de nouveaux prospects et de nouvelles recrues de venir rejoindre la structure. Perspectives intéressantes et peut-être moins chimériques qu'elles peuvent paraître à première vue, sachant que les classements d'avocats et la notation des professionnels sont « *à la mode* », tout comme la mise en place de

78 - À horizon fin 2020, le risque cyber demeure le principal risque et il devrait rester en tête des risques majeurs à l'horizon fin 2024 selon la Fédération Française de l'Assurance (Cartographie 2020 des risques émergents pour la profession de l'assurance et de la réassurance, févr. 2020, www.ffa-assurance.fr).

79 - Voir not. Club des juristes, janv. 2018, Assurer le risque cyber (www.leclubdesjuristes.com).

80 - Cigref, 2016, Le cyber risque dans la gouvernance de l'entreprise (www.cigref.fr).

81 - Ajout de l'art. 1.5 du RIN par déc. CNB, 30 juin 2011, NOR : JUSC1117908S, JO 21 juill.

82 - Barreau de Paris, 2013, Vade mecum de la déontologie du numérique (www.avocatparis.org).

83 - De la même manière que la mise en conformité RGPD des cabinets d'avocat qui, « *outre le gage de confiance qu'elle constitue pour les clients et les collaborateurs, (…) risque fort de devenir un enjeu de positionnement concurrentiel entre les cabinets d'avocat eux-mêmes face aux entreprises qu'elles accompagnent* ». A. Renard, L'impact du RGPD sur les cabinets d'avocats, Lexbase, La lettre juridique, n°750, 19 juill. 2018.

« *cyberscores* »[84]. La cybersécurité serait-elle aussi, pour la profession d'avocat, « *un enjeu commercial méconnu et sous-estimé* »[85] ? « *Associée jusqu'ici à l'idée de contraintes et de dépenses, la cybersécurité doit être considérée aujourd'hui comme un atout compétitif et un investissement productif* »[86]. Raisons suffisantes, s'il en était, de ne pas hésiter à promouvoir et à tirer avantage d'une bonne gestion du risque cyber.

À première vue, il suffisait d'inverser le raisonnement sur les différents impacts d'un incident cyber pour mesurer les intérêts d'évaluer et de réduire son exposition aux risques cyber. Mais il s'avère que s'impliquer dans la cybersécurité et la cyberrésilience du cabinet a des incidences allant bien au-delà de la seule pérennité de la structure d'exercice : apportant une véritable plus-value à l'activité du praticien, replacé au cœur de son écosystème en tant que partenaire de confiance, la sûreté numérique permet aussi de promouvoir les valeurs et principes essentiels de la profession. Les enjeux de la sûreté numérique ainsi évoqués, il reste à se pencher sur la manière dont il est possible d'agir concrètement. Comme nous l'avons vu, les solutions de réduction du risque cyber sont autant techniques (pare-feu, sauvegardes, chiffrement des données, etc.), que liées à la mise en place de processus d'analyse de risques notamment. Elles passent aussi par des actions de sensibilisation et de formation des utilisateurs qui vont permettre d'agir au quotidien pour prévenir les incidents cyber et, plus largement les fuites de données. Les dangers sont nombreux, mais ils peuvent « *être fortement réduits par un ensemble de bonnes pratiques, peu coûteuses, voire gratuites, et faciles à mettre en œuvre au sein du cabinet* »[87].

Aude Dorange

Partie 4 - Mettre en place des mesures d'« hygiène numérique » au sein des structures , à paraître dans le prochain numéro du Journal du Village de la Justice.

84 - Voir par exemple la proposition de loi pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public, qui envisage de « *créer une sorte de "nutriscore" de la cybersécurité des solutions numériques afin que le consommateur ne soit plus démuni* » (Sénat, PP n° 629-19/20, 15 juill. 2020).

85 - Sur cette question, voir le Point de vue de N. Zubinski, « *La cybersécurité, cet avantage méconnu des cabinets d'avocats* », dans ce numéro du Journal du Village de la Justice, p. 38.

86 - CLUSIF-OSSIR, Livre blanc sur La cybersécurité à l'usage des dirigeants (précité).

86 - CLUSIF-OSSIR, Livre blanc sur La cybersécurité à l'usage des dirigeants (précité).

87 - ANSSI-CPME, Guide des bonnes pratiques de l'informatique, 12 règles essentielles pour sécuriser vos équipements numériques (www.ssi.gouv.fr).

Genwin.tech

Tour Montparnasse
75014 PARIS
10 Place du Temple Neuf
67000 STRASBOURG
Mail : contact@genwin.fr
Site Web : genwin.fr

Genwin.tech est une société spécialiste du numérique nouvelle génération et un cabinet de recrutement qui opère dans les domaines de l'IT et de la sécurité de l'information.
Nos équipes accompagnent au quotidien les organisations dans leur évolution, leur transformation et leurs projets structurants.
Notre offre *IT Services* propose d'intervenir sur la définition des besoins (AMOA), le développement *cross-language* et *cross-environment* et la maintenance des grands systèmes.
Notre offre *Information Security* s'attache à déployer les conditions nécessaires pour protéger votre information stratégique et sensible et assurer bonne gouvernance SSI dans un environnement d'incertitude croissante.
Par notre offre *Cabinet de Recrutement*, nous nous occupons également de la recherche de profils à haut potentiel pour aider les entreprises à répondre à leurs ambitions avec les talents dont elles ont besoin.

INGENCOM

Tél : 01 84 73 60 01
Mail : contact@ingencom.com
Site Web : www.ingencom.com

INGENCOM est une société de conseil et prestations de services numériques à destination des entreprises, dotée d'une réelle expertise auprès des cabinets d'avocats.
Forts de notre expérience, nous vous accompagnons dans l'évolution digitale de votre cabinet, pour répondre aux enjeux d'aujourd'hui et de demain alliant sécurité, souveraineté numérique et conformité RGPD.
Nous attachons une grande importance à proposer à nos clients des solutions personnalisées correspondant à la taille et aux objectifs de la structure. Nous sommes soucieux de comprendre vos problèmes et vos attentes afin d'y apporter une solution précise et optimum.
Ne craignez plus les fuites de données ou les attaques de ransomware, nous travaillons avec des acteurs de pointes dans le domaine de la cybersécurité, Françaises pour la plupart.

Contactez-nous pour en savoir plus sur nos offres et bénéficier d'un premier audit informatique de votre cabinet.

NetExplorer

11 boulevard Déodat de Séverac
31770 COLOMIERS
Tél. : 05 61 61 20 10
Mail : contact@netexplorer.fr
Site Web : netexplorer.fr

NetExplorer, solution de partage de fichiers, stockage en ligne et travail collaboratif depuis 2007.

La plateforme NetExplorer vous permet d'échanger en toute confidentialité des documents en interne avec vos collaborateurs, ou en externe avec vos clients. Partagez vos fichiers en toute sécurité et conservez le contrôle de vos données : date d'expiration des partages, protection par mot de passe, droits d'accès avancés (téléchargement ou consultation uniquement), etc.
Accédez à un même espace de collaboration et fluidifiez votre gestion documentaire. Coéditez vos documents et contrats, que vous soyez dans vos locaux, en télétravail ou en déplacement, directement depuis votre navigateur Internet. Les changements de chaque utilisateur apparaissent en temps réel et s'enregistrent automatiquement.
NetExplorer vous garantie une sécurité maximale avec notamment un stockage de vos données en France conforme au RGPD. NetExplorer est certifiée ISO 27001, ISO 14001, ISO 9001, PCI DSS (pour les données bancaires) et HDS (pour les données de santé).

Wolters Kluwer

14 Rue Fructidor
75814 Paris
Tél. : 08 09 10 24 12
Site Web : www.wolterskluwer.com/fr-fr/solutions/logiciels-de-gestion-pour-avocats

Les professionnels du droit doivent faire face à de nouveaux modes de travail et de communication : collaboration virtuelle favorisée, télétravail privilégié, nouveaux besoins technologiques. Avec nos logiciels de gestion pour cabinets d'avocats Kleos et Lop, tous les outils sont à portée de mains : mobilité 24/7, sécurité des données, intégration totale avec les outils Microsoft et Google, bible d'actes Lamy, connexion RPVA, facturation rapide, Extranet client... sur Mac ou PC.

Cette agilité n'est possible que si vous disposez de logiciels de gestion performants et sécurisés. Les serveurs sont hébergés en France et en Allemagne et certifiés aux normes sécurité des données les plus élevées : ISO 27 001, SAS-70 Type II, Norton Secure et McAfee.

Nous n'avons subi aucune perte de données ! Merci de la confiance des utilisateurs qui hébergent quotidiennement leurs données sur nos serveurs et peuvent travailler aujourd'hui en toute sécurité et mobilité !

+ DE 23 000 CLIENTS NOUS FONT CONFIANCE

9 400
COMPTABILITÉS TRAITÉES

6 200
BULLETINS DE PAIE ÉDITÉS

20 000
DÉCLARATIONS VISÉES

6 000
UTILISATEURS LOGICIELS

ANAFAGC

Être client ANAFAGC, c'est profiter d'une offre de service complète qui répond spécifiquement aux besoins de votre cabinet.

COMPTABILITÉ & CONSEIL
9 400 COMPTABILITÉS TRAITÉES
cc@anafagc.fr

Que vous soyez soumis au régime BNC ou BIC, à l'IR ou à l'IS, ANAFAGC vous assiste dans la gestion de votre cabinet : vous accompagne dans le traitement de vos structures connexes (SCI, SCM & SPFPL / holding) et dans votre fiscalité personnelle : vous propose des missions de conseils (prévisionnel, financement d'un investissement, statut du dirigeant, évaluation de fonds, transformation...).

GESTION COMPTABLE ASSISTÉE (BNC)
À partir de 26 €[HT/mois]
Révision de votre comptabilité et établissement de la déclaration 2035 à partir de votre saisie sur notre logiciel AIDAVOCAT COMPTA.

TRAITEMENT GLOBAL (BNC & BIC)
À partir de 48 €[HT/mois]
Saisie de vos pièces comptables et établissement de la déclaration 2035.

AUTRES MISSIONS
Structures connexes, fiscalité personnelle & missions de conseils.

SOLUTIONS LOGICIELLES
6 000 UTILISATEURS
si@anafagc.fr

ANAFAGC vous propose des solutions logicielles spécialement adaptées pour une gestion optimisée de votre cabinet. Conçues pour répondre aussi bien aux besoins des petites et moyennes structures d'avocats. Pour une gestion complète de votre cabinet, AIDAVOCAT COMPTA et GESTION (monoposte ou réseau) sont complémentaires et intégrées. Des prestations techniques ou encore des formations sont disponibles pour accompagner au mieux votre démarrage.

AIDAVOCAT COMPTA | 18 €[HT/mois]
Pour gérer de manière simple et intuitive votre comptabilité.

AIDAVOCAT GESTION | 29 €[HT/mois]
Suivi des dossiers, facturation, RPVA... l'essentiel de votre gestion.

I-COMPTA | 18 €[HT/mois]
Saisie de vos recettes/dépenses en mode Saas.

SERVICES
Installation, aide au démarrage, formation,...

VISA FISCAL
20 000 DÉCLARATIONS VISÉES
vf@anafagc.fr

Agréée par l'administration fiscale, ANAFAGC vous accompagne dans la réalisation de vos obligations fiscales quelle que soit votre activité.

VISA FISCAL | 225 €[HT/an]
Pour bénéficier de la dispense de majoration de 25% du bénéfice imposable.

PASS MICRO | 70 €[HT/an]
Pour bénéficier d'un outil de gestion et d'un accompagnement dans le choix de votre régime d'imposition (micro-BNC ou déclaration contrôlée).

PAIE & MISSIONS SOCIALES
6 200 BULLETINS DE PAIE ÉMIS
pms@anafagc.fr

Pour le traitement de la paie de tous vos salariés, quelle que soit la nature de leurs contrats, nos équipes se chargent de l'élaboration des soldes de tout compte, de la déclaration sociale nominative, de l'application de la convention collective...

BULLETIN DE PAIE | À partir de 20 €[HT]
Pour le traitement de votre bulletin de paie, incluant toutes vos obligations légales et conventionnelles (prélèvement à la source, calcul des indemnités...).

AUTRES MISSIONS
Affiliation aux organismes, assistance en cas de contrôle Urssaf, aide à la décision en matière sociale, gestion de la médecine du travail.

Partenaire de votre cabinet.

ANAFAGC | Association Nationale d'Assistance Fiscale et Administrative, de Gestion et de Comptabilité
5 rue des Cloys, 75898 Paris Cedex 18 | Tel. 01 44 68 60 00 | Fax 01 44 68 61 68 | contact@anafagc.fr | anafagc.fr
SIRET 812 454 247 00014 | TVA intracommunautaire FR 08 812 454 247

ET SI LA CYBERSÉCURITÉ DEVENAIT ENFIN ACCESSIBLE AUX PETITES ET MOYENNES STRUCTURES D'EXERCICE ? ENTRETIEN AVEC FRANS IMBERT-VIER

Il faut bien admettre que la technicité de la sécurisation des systèmes d'information ne rend pas la matière très attractive. Et les enjeux de la protection de la confidentialité des informations gérées par les cabinets d'avocat peuvent la rendre anxiogène. Frans IMBERT-VIER, CEO d'Ubcom[1], société spécialisée dans le conseil en stratégie de cybersécurité, partage avec nous son regard d'expert pour démystifier le sujet et tenter, par la même occasion, de lever les réticences des cabinets d'avocat à monter en puissance dans la protection de leurs données.

© 2018 Glamour Photography Studio by Ph. Jacquot

Journal du Village de la Justice : Tous les cabinets d'avocats sont-ils réellement exposés à la cybercriminalité ?

Frans Imbert-Vier : La réponse est clairement oui. Ils sont tous exposés, mêmes les gros cabinets qui ont des ressources dédiées à la cybersécurité. Il y a des attaques ciblées, qui visent un cabinet en particulier, ainsi que des attaques automatisées, sans filtre : tout le monde prend « *la même dose* » au même moment. C'est d'ailleurs ce qui s'est passé avec l'attaque du parquet de Paris. Ce type d'attaque est ciblée d'un point de vue thématique (le judiciaire), tout ce qui peut être balayé est touché par des automates. C'est souvent pour créer un leurre, la cible réellement visée étant « *noyée dans la masse* ».

« L'avocat est une source d'informations déterminante en termes d'efficacité : autant, en effet, aller prendre l'information là où elle est centralisée… »

Ce n'est pas vouloir provoquer la peur pour le plaisir que de dire que la question n'est pas de savoir si on va être attaqué, mais quand on va être attaqué. On ne parle que des « *gros* », parce qu'ils ont une image de marque à défendre. Mais les « *petits* », eux, ont peut-être mis dix ans à construire cette réputation et elle pourrait être détruite demain en un rien de temps parce qu'ils n'ont pas été bien conseillés. Et il faut bien reconnaître qu'il n'y avait jusqu'ici pas vraiment de solutions adaptées pour protéger les cabinets d'avocats, notamment les petites et moyennes structures. Du moins, pas sans qu'elles aient à investir des sommes non supportables, avec le plus souvent un niveau de performance assez médiocre. La maturité va venir au fur et à mesure.

JVJ : Certains domaines d'activités rendent-ils l'avocat plus vulnérable ?

FIV : Aucun cabinet n'est intouchable, même s'il est vrai que les pénalistes sont probablement les plus sensibles. Mais avec des divorces un peu compliqués par exemple, notamment lorsque des patrimoines importants sont en jeu, il ne faut pas s'étonner que l'une des parties aille voir un hacker pour lui demander d'aller fouiller un peu ! Et l'avocat est une source d'informations centrale, une cible déterminante en termes d'efficacité : autant, en effet, aller prendre l'information là où elle est centralisée… Et pour prendre un autre exemple, les taux de dépôts de bilans liés à une attaque informatique sont très élevés, avec des entreprises qui ne s'en remettent pas. Et avec la crise de la Covid-19, cela risque d'être démultiplié, l'ANSSI ayant signalé une croissance de 200 % du nombre d'attaque depuis la COVID. La compromission d'information est aujourd'hui aussi facile à révéler chez un gros cabinet, que chez un petit.

JVJ : Le coût élevé de la sécurisation des outils et systèmes d'information est souvent avancé pour expliquer l'absence d'investissement budgétaire en la matière. Est-ce que ça coûte vraiment cher de sécuriser ses données ?

FIV : Plus maintenant. Jusqu'ici, ce segment du marché de la cybersécurité, relatif aux petites et moyennes structures, ne se voyait proposer que de la sécurité informatique, c'est-à-dire un simple outil de sécurité informatique, souvent passif, mais pas réellement un accompagnement en cybersécurité.

Mais depuis quelques mois, les acteurs leader du marché de la cybersécurité mondiale proposent en effet des offres « SMB » (*small medium business*),

1 - www.ubcom.eu.

à des coûts unitaires tout à fait supportables pour les petites structures notamment et avec un niveau de protection équivalent à ce que peut s'offrir une entreprise d'un grand groupe.

« Les services de cybersécurité, qui étaient jusqu'ici inaccessibles aux petites et moyennes structures, vont enfin le devenir ».

La commercialisation n'en est qu'à ses débuts, mais c'est un vrai bouleversement. Les services de cybersécurité, qui étaient jusqu'ici inaccessibles aux petites et moyennes structures, vont enfin le devenir. Il est désormais possible d'équiper correctement un cabinet pour quelques dizaines, admettons une centaine, d'euros par mois. C'est une vraie révolution. À ce jour, deux leader mondiaux proposent ces solutions (Sophos et Checkpoint).

JVJ : Et ce type d'offres est-il à même de répondre aux attentes des petites et moyennes structures d'exercice ?

FIV : Elles couvrent en effet tous les besoins techniques : le phishing, la fuite d'informations, le cryptage et le chiffrement, l'espionnage, le vol de données, l'altération des données, les écoutes. De plus, ce sont des offres « *tout-en-un* », compatibles non seulement sur Mac et PC, mais aussi téléphone mobile et avec des business model à la location (sans investissement), à un niveau de performance bien supérieur à ce que proposait le marché il y a encore six mois. Ce qui fait le prix d'un équipement, c'est la puissance capable de gérer tous les flux qui entrent et qui sortent. Une petite organisation a des flux d'informations bien moindre que ceux d'un grand groupe, c'est donc forcément moins cher, mais le logiciel est le même. De plus, ce sont des systèmes qui s'appuient sur des détections de compromission pilotées par l'intelligence artificielle, qui agit rapidement. Et c'est aussi pour cela que l'offre devient abordable : l'humain n'intervient que parce que l'IA lui a signalé le problème, qui a déjà été stoppé. C'est inégalé en termes de compétitivité.

Cela reste un coût, même relativement modeste, il faut bien le reconnaître. Mais il faut aussi garder à l'esprit que ce n'est plus vraiment une question d'argent : l'impact sur la violation d'une compromission d'informations pour un avocat vaut évidemment mille fois plus que les frais d'abonnement chez un prestataire de confiance.

JVJ : En ce qui concerne le choix des prestataires et des outils numériques, auriez-vous quelques conseils ?

FIV : Il faut d'abord faire tomber un tabou et ne pas avoir peur de valoriser certaines marques, surtout si ce sont des marques françaises et européennes et ne pas forcément s'appuyer sur les gros acteurs. Sous prétexte qu'ils sont connus, ce ne sont pas forcément les meilleurs. Soyons nationaliste ou européaniste sur la technologie : quand, enfin, on a des produits qui marchent, des solutions sont matures, il ne faut pas hésiter à se tourner vers eux, même si elles sont parfois un peu plus chères ! Commencer par utiliser une visio-conférence souveraine et chiffrée comme Tixeo ou le transport chiffré de vos documents avec Seald. Ce n'est pas gratuit bien sûr, mais c'est sérieux, efficace et, en plus, cela permet de se conformer à l'article 32 du RGPD incitant à une obligation de sécurisation du système d'information.

En ce qui concerne les prestataires en cybersécurité, il faut s'assurer qu'il soit certifié (ou qui s'appuie sur l'expertise d'un partenaire certifié), qui a une vraie maîtrise du produit et qui saura mettre en avant sa pertinence dans le cadre du métier du client final. Plus que la mise en place de techniques de sécurité informatique, c'est l'élaboration d'une véritable stratégie de sécurisation qui va être proposée, en parfaite adéquation avec les attentes du cabinet.

Pour les outils, beaucoup de critères peuvent être pris en compte. Il peut toujours être utile de se renseigner sur la nationalité de l'entreprise, son lieu de domiciliation, la nationalité de ceux qui détiennent les capitaux, le lieu d'hébergement des données ou bien encore les mesures de cybersécurité qui sont mises en place au sein de l'entreprise. Il faut bien garder en mémoire que si l'avocat n'est pas responsable du vol d'informations qui les concerne chez un tiers à qui il a sous-traité une prestation, il reste responsable du stockage de cette information et de son envoi.

Il ne faut donc pas hésiter à se renseigner, au besoin en faisant appel à des cabinets un peu experts, qui ont une très bonne connaissance du marché des acteurs de la cybersécurité, surtout quand il s'agit de souveraineté.

Propos recueillis par Aude Dorange

L'AUDIT CYBER POUR LES CABINETS D'AVOCATS : COMMENT ET POUR QUOI FAIRE ?

Dans le cadre de la protection de l'information, la démarche d'audit représente cette opportunité de prendre conscience de ses lacunes, mais surtout de gérer ses efforts et ses investissements de manière plus efficiente. Force est cependant de constater que cette pratique, malgré ses bénéfices, est moins répandue qu'elle ne le mériterait, en raison de plusieurs sources d'incohérence et de confusion, dont il faut se débarrasser. Explications de Mathieu MEYER, Cofondateur-Directeur associé de Genwin.tech et Expert en risques informationnels, sûreté et cybersécurité.

Mossack Fonseca, Grubman Shire Meiselas & Sacks ou les 50 autres cabinets visés par le cybercriminel Oleras sont autant d'exemples que les cabinets d'avocats ne sont pas épargnés par les fuites de données. Dans un contexte d'incertitude où le risque zéro n'existera jamais, rien ne garantit que ces incidents ne se seraient pas produits dans le futur, malgré des actions sécuritaires supplémentaires. Cependant, en sachant que plus de 30% des fuites d'informations[1] proviennent d'expositions par inadvertance des données (e.g. erreurs de configuration, exposition involontaire, incompétence), il paraît évident qu'il est possible de réduire significativement les risques d'incidents en adoptant quelques pratiques simples mais structurantes sur lesquels chacun peut agir. Et cela commence par prendre conscience de ses propres vulnérabilités, une attitude proactive et responsable qui ne passera pas inaperçue auprès de clients pour qui la confiance est indispensable.

La spécificité de la profession d'avocat et la recrudescence des menaces liées à l'information sont des faits dont la prise de conscience devrait motiver tout professionnel du domaine à s'interroger sur ses propres pratiques de protection de l'information sensible.

Avec 15,1 milliards de données volées[2], 2019 aura marqué une nouvelle fois un record, tristement battu d'année en année. La fuite de données reste bien l'un des types d'incident les plus répandus et les plus impactant pour les organisations, connaissant une progression annuelle tout à fait remarquable (+ 284 %). À ceux qui se disent qu'ils n'intéressent personne ou qui se posent encore la question de savoir qui peut bien s'en prendre à leurs données, tout laisse à penser qu'il n'a jamais été aussi probable que réponse leur soit faite prochainement, à leurs dépens.

Du fait de la nature-même de ses activités, la profession d'avocat reconnaît la confidentialité comme un besoin intrinsèque et intangible. Peu de corps de métier bénéficient en effet d'une reconnaissance normative de l'obligation de protéger l'information qui leur est confiée et qu'ils échangent. Et si, plus qu'un impératif, la protection du secret professionnel devenait aussi un avantage concurrentiel et un gage d'excellence ?

Cette question, contre-intuitive de prime abord, interroge pourtant sur les notions de confidentialité et de confiance, à l'heure du virage numérique et de l'utilisation généralisée des moyens informatiques. Le secret professionnel s'applique de manière « *général, absolu et illimité dans le temps* » aux informations et aux échanges client-avocat et entre avocats, « *quels qu'en soient les supports, matériels ou immatériels* »[3]. Si cette règle est claire, ses conséquences sur les pratiques professionnelles au quotidien sont cependant parfois mal appréhendées, menant à l'émergence de nouvelles sources de vulnérabilités liées aux nouvelles technologies.

Pour réconcilier les bénéfices d'une technologie devenue aussi appréciée qu'indispensable et les exigences de confidentialité de la profession d'avocat, la réappropriation des enjeux de sécurité est incontournable.

Mais connaître et maîtriser les subtilités d'un domaine parfois complexe et abstrait, souvent immatériel et technique, échappe

1 - VERIZON, *Data Breach Investigations Report*, 2020
2 - *RiskBased Security*, 2019 *Year End Report Data Breach QuickView*
3 - Art. 2 du Règlement Intérieur National de la profession des avocats (RIN), relatif au secret professionnel.

d'ordinaire aux professionnels du droit. Tout comme d'ailleurs, à l'identique, la finesse et l'intelligence du droit peut échapper aux non-initiés. Le recours aux sachants devient alors un choix judicieux pour se faire accompagner et permettre de prendre des décisions pertinentes, éclairées et rentables.

L'audit de cybersécurité n'est ni réservé aux grands groupes, ni une entreprise d'inquisition des pratiques habituelles au sein de la structure considérée. En quoi consiste la démarche exactement ?

Deux types d'audit peuvent ici être distingués. D'une part, l'audit de conformité, qui revêt souvent un caractère obligatoire et vise à prouver à un tiers le respect de règles définies et admises (*e.g.* norme, standard, règlement, certification). Il est source de garantie pour ce tiers et d'uniformisation des pratiques. D'autre part, l'audit d'amélioration volontaire provient plutôt d'une initiative choisie par l'entité qui, ayant compris que la robustesse de son fonctionnement interne est bénéfique pour elle-même et ses clients, le transforme en un avantage concurrentiel immédiat. Ce type d'audit est source de confiance car la proactivité de la démarche indique l'attention portée aux questions de protection de l'information.

« Ce type d'audit est source de confiance car la proactivité de la démarche indique l'attention portée aux questions de protection de l'information ».

Pour en tirer tous les avantages et rationnaliser ses coûts, il est important de penser sa stratégie d'audit à long terme en respectant quelques principes élémentaires : travailler progressivement / par priorité ; définir l'objectif / l'effet attendu de chaque audit ; définir son périmètre ; informer et impliquer les collaborateurs et les salariés du cabinet.

L'effort premier pour définir sa stratégie d'audit consiste à prioriser les chantiers à traiter, c'est-à-dire ceux dont les bénéfices seront les plus forts. Pour ce faire, la réalisation d'une analyse de risques portant sur la sécurité de l'information est probablement le meilleur choix possible. En prenant conscience des éléments critiques pour son activité, il devient plus simple d'appréhender les conséquences, soient-elles opérationnelles, financières, juridiques ou réputationnelles par exemple, auxquelles un cabinet d'avocats s'expose en cas d'incident de sécurité.

L'exercice consiste à mener trois phases successives répondant, chacune, à des buts précis :

(1) Quels sont les éléments informationnels indispensables pour mener mon activité ?
(2) Quels risques pèsent sur eux ?
(3) Quelles actions mener pour réduire ces risques ?

La démarche fait alors appelle à une évaluation croisée : l'une portant sur les besoins en sécurité de l'information, dans toutes ses formes, par des critères de disponibilité, d'intégrité, de confidentialité et de traçabilité ; l'autre sur la gravité et la probabilité d'occurrence des incidents. Cette approche, bien menée, a ainsi la capacité d'identifier de manière méthodique les axes prioritaires sur lesquels concentrer les efforts en matière de sécurité, car indispensables à la poursuite des activités.

L'identification des chantiers prioritaires apparaît alors naturellement. Dans cette situation, la démarche d'audit peut enfin être rationnalisée, maîtrisée et revenir à portée de tous, car :

- Les périmètres d'études sont définis et priorisés, permettant de procéder à des actions d'audit ciblées ;
- La stratégie d'audit peut se construire sur une approche progressive, logique et de bon sens ;
- Les efforts peuvent être concentrés au lieu d'être dispersés ;
- Les interdépendances entre les acteurs du système d'informations sont identifiées, mettant à jour l'étendue réelle de notre responsabilité en matière de protection de l'information[4].

4 - Rappelons que les sous-traitants sont des cibles fréquentes d'attaques et que le RGPD considère une responsabilité partagée en cas de fuite de données due à un manque de moyens de protection (art. 82).

La démarche d'audit souffre parfois d'une image de pratique imposée, coûteuse et inabordable pour les petites et moyennes structures d'exercice professionnel. Il est pourtant essentiel de rendre la démarche plus accessible et plus utile.

Rappelons tout d'abord qu'il s'agit très fréquemment d'une démarche volontaire. Il est essentiel pour tout cabinet d'avocats, sans considération de taille ou de spécialisation, de se réapproprier les enjeux-mêmes de son métier : être crédible en offrant tous les moyens nécessaires à la protection des intérêts de ses clients. Procéder à une analyse de risques doit aider à répondre à cet objectif, en identifiant clairement les actifs les plus essentiels à la poursuite de l'activité, en estimant les risques actuels pesant sur ces derniers et en identifiant les mesures d'amélioration nécessaires pour renforcer leur préservation.

Le choix d'un audit ne doit pas être hasardeux ; il s'agirait là du meilleur moyen d'alimenter les travers classiques reprochés à cette pratique : une dérive des coûts, un résultat peu exploitable ou un sentiment de « *flicage* » partagé chez les audités. Nous comprenons alors qu'au-delà des certifications ou de l'expérience, le bon analyste de risques, et par extension le bon auditeur, sera toujours celui qui cherche à comprendre le métier, pour mieux identifier ce qui lui importe le plus et comprendre comment il fonctionne. Chacun se doit de donner du sens à son action en restant au service des Métiers. La pratique nécessite simplement d'en refaire un moyen et non une fin en soi.

« Le bon auditeur sera toujours celui qui cherche à comprendre le métier, pour mieux identifier ce qui lui importe le plus et comprendre comment il fonctionne ».

Sa mauvaise réputation, l'audit cyber la doit vraisemblablement à l'inadéquation des propositions faites par certains professionnels de l'audit et à des objectifs trop flous. Pourtant, en tant qu'observateur extérieur, l'auditeur dispose d'avantages indéniables : neutralité, impartialité, objectivité des analyses et regard critique sur des modes de fonctionnement en vigueur.

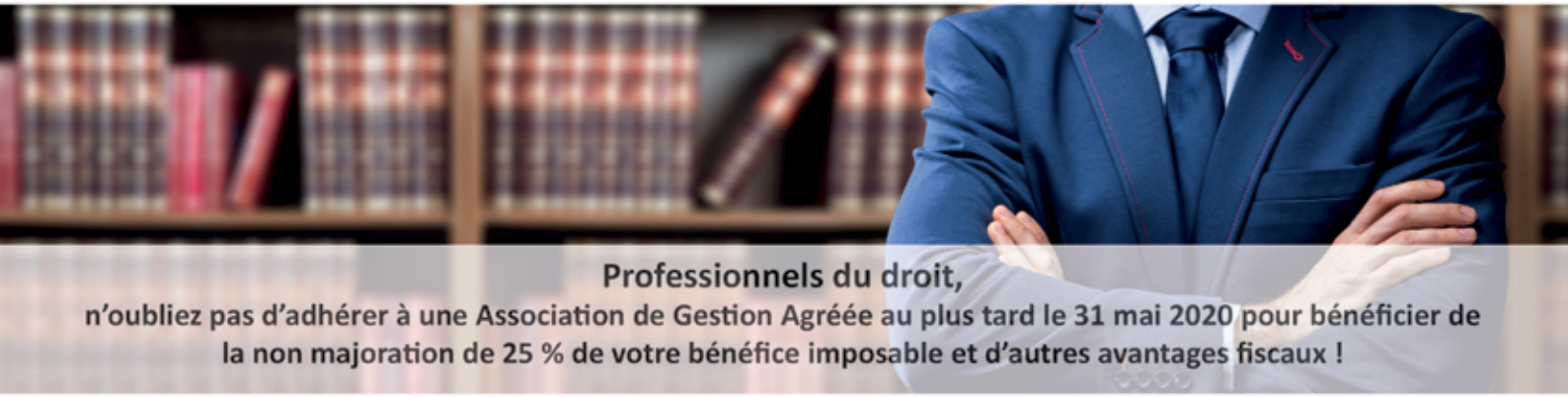
La priorisation qui découle de l'analyse de risques[5] est probablement l'un des facteurs clés de la réappropriation de la démarche d'audit. Pour être utile, celle-ci doit être adaptée au contexte et aux besoins de chaque cabinet. La valeur ajoutée de la démarche ne se mesure pas uniquement à la méthode utilisée ou au temps passé, mais aussi à la capacité des auditeurs à comprendre son client, son environnement et ses enjeux pour proposer une approche construite, personnalisée et progressive. Ainsi est-il judicieux de ne pas s'interdire de solliciter plusieurs prestataires d'audit, incluant des « *outsiders* » dont la taille réduite peut présenter des avantages de flexibilité et de coût, et de comparer les propositions au regard du prix, peut-être, mais surtout de la pertinence des actions envisagées.

5 - Voir *supra*.

AGA FRANCE

L'AGA DES PROFESSIONS LIBERALES

ASSOCIATION DE GESTION AGREEE DEPUIS 1998



Professionnels du droit,
n'oubliez pas d'adhérer à une Association de Gestion Agréée au plus tard le 31 mai 2020 pour bénéficier de la non majoration de 25 % de votre bénéfice imposable et d'autres avantages fiscaux !

Vous êtes professionnel libéral du droit, avez-vous choisi le régime fiscal le mieux adapté à votre situation et à vos résultats ? L'AGA FRANCE répond à toutes vos questions !

Qu'est-ce qu'une AGA (Association de Gestion Agréée) ?

Une AGA est une association à but non lucratif agréée par l'Administration Fiscale. Elle a pour mission d'accompagner ses adhérents (professions libérales) dans la gestion de leur comptabilité et leurs obligations fiscales et de leur faire bénéficier de plusieurs avantages fiscaux si leur régime fiscal est celui de la déclaration contrôlée. L'administration fiscale vérifie régulièrement que l'organisme de gestion agrée accomplit les missions qui lui sont confiées et répond aux différentes questions de ses membres adhérents. L'AGA est tenue de respecter un certain nombre d'obligations administratives auprès de l'Administration Fiscale.

Quand adhérer ?

- Je crée mon activité ou je l'ai créée en cours d'année : **Vous devez adhérer dans les cinq mois suivant la date de début d'activité.**
- C'est ma première adhésion à une association de gestion agréée : **Vous devez adhérer au plus tard le 31 mai de l'année pour laquelle vous souhaitez bénéficier de la non majoration de 25 % de votre bénéfice imposable.**
- Je suis déjà membre d'une AGA : **Vous devez adhérer à l'Aga France dans les 30 jours de la date d'effet de démission de votre ancienne AGA.**

Avantages de l'adhésion à une AGA :

- **Non application d'une majoration de 25 % du bénéfice imposable à l'impôt sur le revenu**
- **Une réduction d'impôt pour frais d'adhésion et de tenue de comptabilité**

Les adhérents concernés sont uniquement ceux dont les recettes n'excèdent pas le seuil du régime du micro BNC et optent pour le régime de la déclaration contrôlée. Cette réduction est égale à 2/3 des frais d'adhésion et de tenue de comptabilité, plafonnée à 915 €.

- **Dispense de pénalités**

Lors de l'adhésion à une AGA, il est possible d'exercer dans les 3 mois de l'adhésion un droit de repentir auprès de l'administration fiscale, pour les adhérents qui révèlent spontanément les insuffisances de leurs déclarations antérieures.

Pour plus d'informations, rendez-vous sur www.aga-france.fr
ou appelez-nous au 0810 00 20 63

LA CYBERSÉCURITÉ, CET AVANTAGE CONCURRENTIEL MÉCONNU DES CABINETS D'AVOCATS

Le rapport de la mission « Perben »[1], comme d'autres avant lui[2], formule des propositions sur l'avenir de la profession d'avocat qui intègrent très largement l'analyse du marché du droit et des perspectives de développement du « legal business ». Indépendamment du clivage profond que provoque l'analyse économique des activités des professionnels du droit, « tous les acteurs qui offrent des services juridiques, en particulier les avocats et leurs organisations professionnelles, savent bien qu'ils opèrent dans un environnement concurrentiel »[3]. La cybersécurité ne serait-elle pas en passe de devenir un avantage concurrentiel pour les avocats ? Gage de professionnalisme, la cybersécurité devient surtout un moteur de restructuration du marché. Tel est en tout cas le point de vue de Nicolas ZUBINSKI, Expert en stratégie et intelligence économique.

1 - Mission relative à l'avenir de la profession d'avocat, Rapp. au garde des Sceaux, juil. 2020 (www.justice.gouv.fr).
2 - Voir notamment le rapport « Darrois », Mission sur les professions du droit, Rapp. au Président de la République, mars 2009 (www.justice.gouv.fr).
3 - G. Canivet, Les marchés du droit, rapp. Introductif, RIDE 2017/4 (t. XXXI), p. 9 et s.
4 - Rapport Perben, *op. cit.*
5 - Sur la segmentation très particulière du marché français des cabinets d'avocats, voir notamment C. BESSY, Organisation des cabinets d'avocats et marchés des services juridiques, Revue d'économie industrielle, vol. 155, n° 3, 2016, p. 41 et s.
6 - ANSSI & CPME, Guide des bonnes pratiques de l'informatique : 12 règles essentielles pour sécuriser vos équipements numériques, version 1.1.1., sept. 2017 (www.ssi.gouv.fr).
7 - ANSSI, Recommandations sur le nomadisme numérique, version 1.0, 17 oct. 2018 (www.ssi.gouv.fr).

« *La conviction que le droit n'est pas une simple marchandise n'impose (…) pas obligatoirement d'ignorer les règles du marché, ou d'imaginer qu'on peut y échapper* »[4]. Or, la grande majorité du marché des cabinets avocats est constitué de structures d'exercice équivalentes, en taille, à des TPE-PME[5]. Leurs capacités d'investissement et fonctions supports sont réduites. Et, dans ce contexte, la cybersécurité est souvent perçue comme un énième centre de coût.

Il importe donc, pour commencer, de se débarrasser d'une croyance communément partagée, selon laquelle la sécurité informatique, et plus généralement celle de l'information, serait coûteuse. Or tel n'est pas forcément le cas. Prenons deux hypothèses usuelles, la protection contre les atteintes aux outils de production puis la fuite d'informations critiques. Dans le premier cas, la sécurité s'acquiert essentiellement par l'adaptation des comportements humains aux risques inhérents de l'environnement informatique. Ce qui s'avère peu onéreux et particulièrement efficace. Ainsi, maintenir une bonne hygiène numérique permet d'atteindre un seuil acceptable de protection. L'application des guides de l'Agence nationale de la sécurité des systèmes d'informations (ANSSI) relatifs aux « *bonnes pratiques de l'informatique* »[6] et au « *nomadisme numérique* »[7] permet, à elle seule, de considérablement réduire l'exposition des cabinets d'avocats aux cyber-attaques. Dans le second cas, pour prévenir le risque de divulgation des informations détenues par les cabinets d'avocats, notamment couvertes par le secret professionnel, le recours à des technologies de chiffrement permet de neutraliser les possibilités d'exploitation de fuites d'informations (celles-ci rendant les données illisibles pour toute personne ne disposant pas de la clé de déchiffrement). Or les technologies de chiffrement à des fins professionnelles sont, elles-aussi, peu onéreuses. Elles permettent en outre de protéger aussi bien les canaux de communications, que les documents de travail (brouillon de jeu d'écritures, dossier de plaidoirie ou de preuve, stratégie de négociation, compte rendu d'investigation, etc.). En somme, un investissement bien modeste, pour un large champ d'application et d'importants effets bénéfiques.

« La cybersécurité est pour la profession d'avocat un enjeu commercial méconnu et sous-estimé ».

Pour saisir ces enjeux, il faut en revenir au secret professionnel de l'avocat. Cette obligation se fonde sur la détention, par les avocats, d'informations qui sont critiques pour les intérêts de leurs clients et dont la confidentialité doit être impérativement préservée. Par conséquent, la capacité des cabinets à déployer et à utiliser convenablement des environnements virtuels sécurisés se révèle être une garantie de mise en œuvre du secret professionnel. Alors, le paradigme s'inverse : il ne s'agit plus (seulement) pour l'avocat de se protéger d'une menace hypothétique, mais surtout d'exploiter un avantage qualitatif dans une démarche de *business development*.

Grâce à la cybersécurité, les cabinets d'avocats – peu important la taille de la structure – vont pouvoir renforcer leur image de marque et se créer de nouvelles opportunités (dossiers à plus forts enjeux

stratégiques ou particulièrement médiatisés). Or, il est piquant de constater que cette profession n'offre toujours pas, dans sa très large globalité, des standards de sécurité informatique et informationnelle satisfaisant au regard de la criticité des informations qu'elle manipule. Sachant que l'*intuitu personae* et le capital réputationnel sont des facteurs clefs du choix d'un avocat, la cybersécurité s'avère être un enjeu commercial méconnu et sous-estimé. Pourtant, elle est un critère décisionnel pour le client, d'autant plus présent dans les secteurs d'activités manipulant de l'information à haute criticité, au sein desquels se développent de manière croissante des écosystèmes de confiance. L'avocat y prend une place particulière du fait des impératifs et garanties liés au secret professionnel. C'est pourquoi - rappelons-le, quelle que soit la taille de la structure -, les cabinets adoptant des standards élevés de protection de l'information pourront accéder à de nouvelles niches et accéder à des affaires pour lesquels les taux de marge sont plus élevés. La cybersécurité est à ce titre un moyen peu coûteux d'élargir son réseau d'affaires et d'accéder à de nouveaux profils de clientèle et d'accroître ses honoraires.

« Les cabinets adoptant des standards élevés de protection de l'information pourront accéder à de nouvelles niches ».

Il s'agit d'évacuer le prisme sécuritaire qui occulte l'intérêt commercial de la cybersécurité. La cybersécurité est aujourd'hui un moteur de restructuration du marché de la prestation juridique. Le regain de sensibilité du marché de la prestation juridique aux risques informatiques et informationnels s'exprime par des indices profondément impactants. Il se concrétise par l'évolution, d'une part, des régimes de couverture en cyber-assurance et, d'autre part, des pratiques d'achats de prestations juridiques chez les professionnels. Prenons spécifiquement le cas de l'émergence du *cyber-rating*, c'est-à-dire de la notation des standards informatiques appliqué par une organisation. Elle est de nature à impacter directement le régime de cyber-assurance[8] en fournissant aux assureurs des outils d'évaluation et de notation de la maturité informatique de leurs assurés. Ce faisant, le cyber-rating favorise l'introduction de nouvelles clauses d'exonération de garantie dans leur police d'assurance. Et, ceci, notamment en visant la négligence de l'assuré (ou de ses préposés) ou l'insuffisance manifeste des moyens de protection de la donnée...

« Si la notation financière des cabinets d'avocats impacte peu le processus décisionnel de leur client, la notation cyber, elle, le sera bien davantage ».

L'augmentation constante de la cybermenace et sa diversification font de la cyber-assurance un enjeu financier ne pouvant plus être négligé. Outre les assureurs, les cabinets d'avocats eux-mêmes ne tarderont pas à se voir imposer des standards de notation cyber. Si la notation financière des cabinets d'avocats impacte peu le processus décisionnel de leur client, la notation cyber, elle, le sera bien davantage. En effet, plus les conditions de couverture des cyber-assurances se durcissent, plus la cybersécurité devient un paramètre de contractualisation pour les entreprises. Et ceci devrait conduire à une modification de leurs politiques achats et, en conséquence, faire de la cybersécurité un critère pertinent d'éligibilité des candidatures dans les appels d'offre des prestations de conseil juridiques.

8 - Sur ce point, voir J.-M. BARBIER, L'autonomie stratégique face au cyber-rating : une nouvelle dépendance émerge… , École de pensée sur la guerre économique, 8 juin 2020 (www.epge.fr).

METTRE EN PLACE UNE STRATÉGIE PATRIMONIALE

Gérer son patrimoine implique bien sûr de chercher à en retirer la meilleure rentabilité. Mais cela consiste surtout à mettre en œuvre une stratégie adaptée à ses objectifs de vie. La mise en place d'une stratégie patrimoniale comporte de nombreux aspects, juridiques bien sûr, mais aussi financiers ou bien encore liés à la situation personnelle du client. Pour l'avocat, il faut parfois beaucoup de temps pour réussir à obtenir l'intégralité des informations nécessaires pour bâtir la stratégie patrimoniale. Et dans des affaires complexes, il peut être assez compliqué, pour l'avocat non spécialisé, de répondre à toutes les attentes de son client. Travail en équipe pluridisciplinaires et interprofessionnalité prennent alors tout leur sens. Mais encore faut-il accompagner le client dans la mise en place de cette offre commune de services. Qu'il s'agisse de préserver sa réputation professionnelle en cas d'apport d'affaires à un autre professionnel du patrimoine ou d'impliquer son client dans la préparation de son dossier, faire preuve de pédagogie est essentiel. C'est dans cette perspective de faciliter la gestion de la relation-client, que nous vous proposons cet article, qui devrait permettre à vos clients de faire eux-mêmes le point sur les trois étapes indispensables pour prendre les bonnes décisions.

Que celui qui n'a jamais résumé la gestion de son patrimoine à la souscription d'un placement jette aux autres la première pierre. Pourtant, la recherche du meilleur produit d'investissement n'est que la dernière étape dans la construction d'une stratégie patrimoniale adaptée et efficace. Car l'argent et l'épargne sont avant tout des outils au service de projets de vie. C'est pourquoi la définition d'une telle stratégie est en fait composée de trois étapes.

La première d'entre elles consiste à réaliser un état des lieux de sa situation actuelle. Si cela peut sembler fastidieux, c'est en réalité indispensable. De nombreux aspects sont à prendre en compte : juridiques (situation matrimoniale notamment), fiscaux (taux d'imposition faible ou élevé), financiers, personnels (personnes à charge, évolution prévisible de carrière), etc.

Phase 1 : les bilans

Pour démarrer, il faudra *a minima* établir deux bilans assez simples.

Premier bilan : l'état des lieux précis de son patrimoine.
D'un côté, les actifs : cela inclut l'immobilier bien sûr, dont la résidence principale mais aussi l'immobilier locatif le cas échéant. Si vous êtes engagé dans un programme de défiscalisation, notez les obligations de durée de location que vous devez respecter et l'année où vous en serez libéré. Pour rappel, si vous avez constaté un déficit foncier (imputé sur le revenu global), veillez à maintenir le bien en location pendant trois ans après la constatation du déficit. Idéalement, estimez aussi la rentabilité de vos biens (même grossièrement) en rapportant le loyer annuel minoré des diverses charges au prix du logement.

De l'autre côté, les actifs financiers : veillez à ne rien oublier, des livrets bancaires au plan d'épargne en actions (PEA) en passant par les assurances-vie. Tenez compte également des enveloppes d'épargne salariale et d'actionnariat salarié que vous pourriez avoir. Là encore, dans la mesure du possible, notez les dates de disponibilité des fonds (dans un livret l'argent est disponible immédiatement mais dans un dispositif d'épargne salariale il est parfois bloqué jusqu'au départ à la retraite).

Enfin, bien sûr, il conviendra d'intégrer le passif, c'est-à-dire les dettes. Il s'agira essentiellement de crédits immobiliers.

Deuxième bilan : le budget.
Ce dernier est finalement plus complexe à mener car peu de gens ont une vision claire sur ce qu'ils dépensent et épargnent réellement. Connaître sa capacité d'épargne est pourtant un point central pour prendre les bonnes décisions patrimoniales.

Du côté des revenus, il faut prendre en compte les salaires et traitements bien sûr mais aussi, lorsqu'ils existent, les revenus des placements (dividendes, loyers...) et les allocations.

Du côté des dépenses, ne pas omettre l'entretien de la maison, les assurances, les frais de scolarité, les impôts, les mensualités de crédit, et tous les frais courants. Attention, il est très fréquent les sous-estimer les dépenses du quotidien (alimentation, sorties, vacances, coiffeur...).

La différence entre les deux résultats vous renseignera sur votre capacité actuelle d'épargne.

Phase 2 : les objectifs.

La première étape étant accomplie, il est désormais temps de déterminer vos objectifs et votre horizon de temps, tout en tenant compte de vos contraintes.

Il est tout à fait possible de cumuler plusieurs objectifs avec des échéances différentes. Par exemple, bâtir un apport personnel pour l'acquisition de sa résidence principale sous deux ans, tout en épargnant régulièrement en prévision de sa retraite. Cette étape est l'occasion de coucher noir sur blanc ses préoccupations, contraintes, interrogations, besoins. Ce n'est pas toujours évident et faire appel à un tiers à ce stade (voir ci-après) peut permettre de révéler des besoins qui jusqu'ici, étaient encore non ressentis.

Il existe des objectifs récurrents d'une famille à l'autre. Parmi les plus fréquents : aider ses enfants (leur préparer un capital pour financer des études ou le démarrage dans la vie active, anticiper sa transmission...), protéger son conjoint (notamment en cas de différences significatives de revenus), dégager des revenus complémentaires (à la retraite, lors d'une reconversion professionnelle, pour profiter de la vie...), mettre sa famille à l'abri du besoin (acheter sa résidence principale, mettre en place une épargne de précaution, épargner en vue de la retraite...).

Ces éléments étant posés, il reste à passer à la phase du diagnostic.

Phase 3 : le diagnostic.

L'objectif est d'identifier les moyens de passer de la situation actuelle à celle souhaitée. Dans les cas les plus classiques, il est tout à fait possible d'être autonome, à condition d'accepter de passer un minimum de temps à s'informer. Mais certains cas de figure peuvent être délicates à traiter seul, lorsque la situation est complexe (famille recomposée par exemple, montages complexes...) ou les enjeux financiers importants (patrimoine conséquent, héritage...). Le recours à un professionnel pour vous orienter est une bonne idée, tout le monde ne peut pas être un fin connaisseur de l'ingénierie patrimoniale et de ses subtilités.

Plusieurs experts peuvent vous accompagner selon vos problématiques. Il sera même parfois indispensable d'être accompagné par plusieurs de ces spécialistes du patrimoine. Pour des questions simples, il est possible de faire appel à votre banquier, voire à un banquier privé qui aura plus d'outils (recours ponctuel à des ingénieurs patrimoniaux, des fiscalistes maison) pour vous aider. Experts-comptables et commissaires aux comptes seront aussi sollicités selon votre situation. Un notaire peut également être de bon conseil, pour des sujets juridiques ou des montages

financiers. Son accompagnement sera même indispensable si la gestion de votre patrimoine suppose la réalisation d'un acte authentique, par exemple en cas de vente immobilière ou de changement de régime matrimonial, qui serait recommandé pour isoler les patrimoines lorsque l'un des conjoints crée une entreprise. S'il s'agit de gérer la dimension fiscale des opérations envisagées ou de prendre en charge un contentieux, c'est l'avocat qui aura un rôle déterminant. Coutiers en crédits et en assurances vous permettront de trouver les meilleures conditions contractuelles. Et pour un accompagnement global et l'orientation vers les experts juridiques et financiers qualifiés, un très bon interlocuteur sera le conseiller en gestion de patrimoine. Ce dernier pourra aussi vous accompagner dans les phases de diagnostics comme dans la mise en place de votre stratégie.

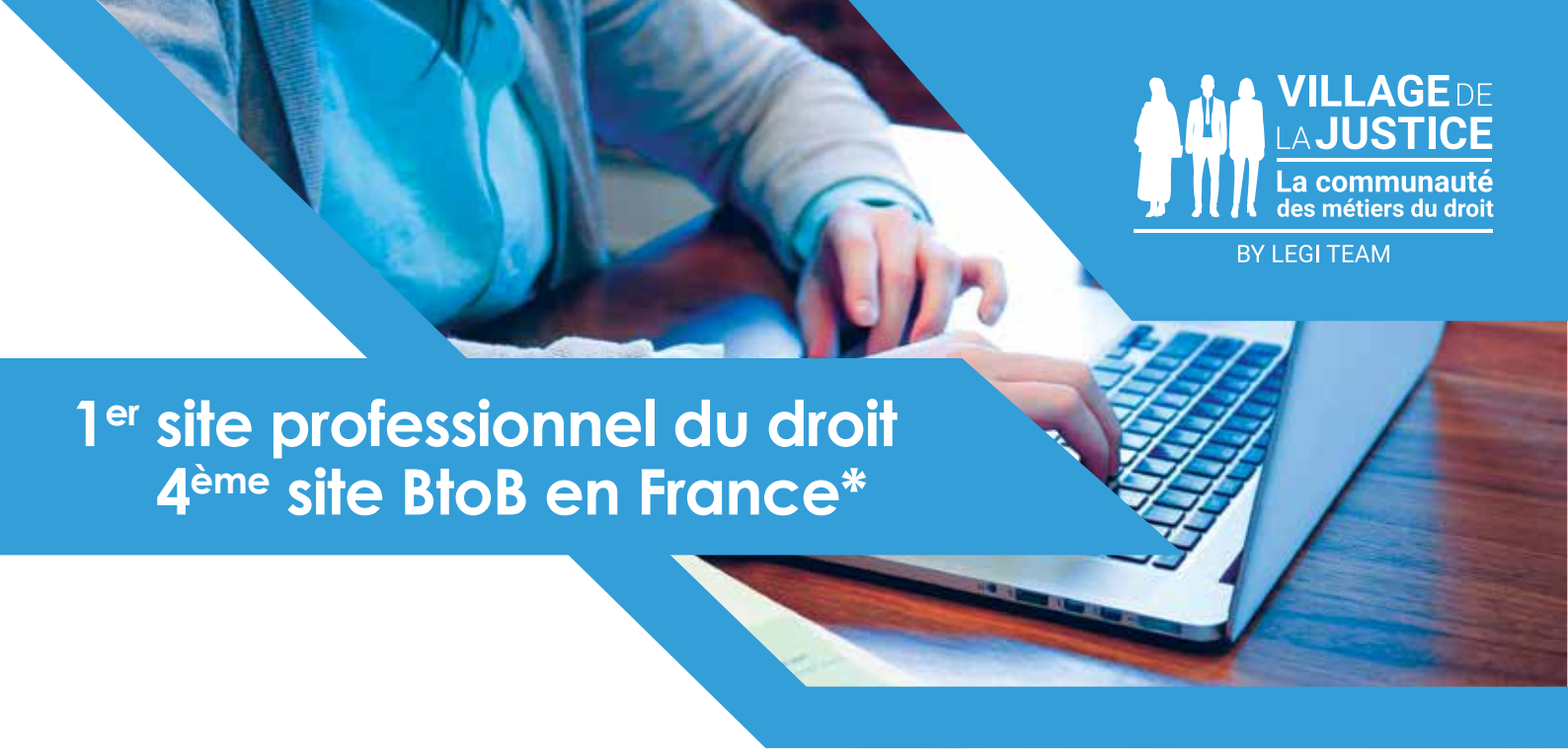
Phase 4 : le choix des produits financiers.

La dernière étape de la construction de sa stratégie patrimoniale consiste à choisir les bons produits financiers : assurance-vie, société civile de placement immobilier (SCPI), épargne-retraite... Pourquoi cette étape arrive-t-elle en dernier ? Globalement, parce que le meilleur produit de sa catégorie, s'il n'est pas adapté à vos besoins, ne sera d'aucun intérêt. Cette dernière étape ne doit donc pas être laissée pour compte. D'autant que, bien souvent, il existe un gouffre entre les meilleurs placements et les pires. C'est particulièrement vrai avec le produit d'épargne phare des Français, à savoir l'assurance-vie. Des centaines de contrats sont commercialisés et il est indispensable de trier le bon grain de l'ivraie.

Si chaque produit a ses propres caractéristiques, une ligne directrice doit vous guider : un bon placement est solide (société de gestion ou assureur réputé), répond à vos besoins (simple ou plus sophistiqué selon votre appétence à la matière) et présente un niveau de frais raisonnable eu égard au service rendu. Dans un environnement où la rentabilité des placements est globalement faible, les frais jouent en effet un rôle crucial sur la durée. Les contenir est donc l'un des outils clés de l'épargnant soucieux d'optimiser son patrimoine.

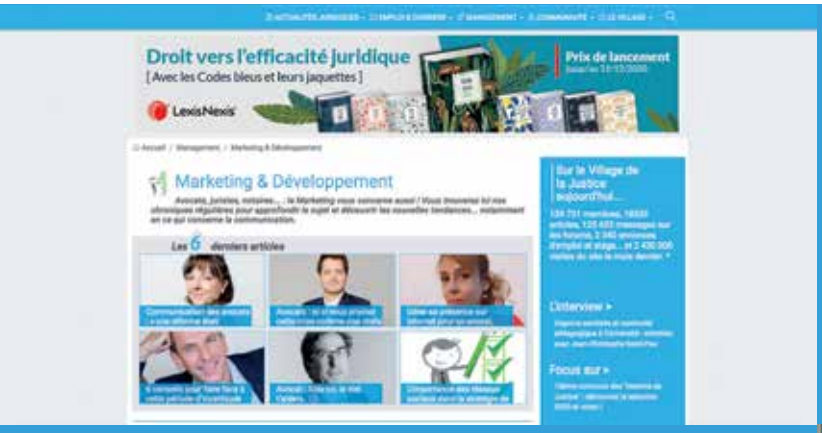
Enfin, gardez en tête que votre situation et vos objectifs vont immanquablement changer tout au long de votre vie. Votre patrimoine devra donc évoluer avec eux. Une stratégie n'est donc jamais figée. Surtout, elle ne doit pas vous freiner dans vos projets.

Aurélie Fardeau



VILLAGE DE LA JUSTICE
La communauté des métiers du droit
BY LEGI TEAM

1er site professionnel du droit
4ème site BtoB en France*



Tous les mois :

2 000 000 de visites*

+ de 10 000 articles d'actualité juridique chaque année
+ des articles en management des métiers du droit

ESPACE RECRUTEMENT

+ de 12 000 CV*
+ de 3 800 annonces d'emploi et de stage*

POUR RECRUTER LES MEILLLEURS ÉQUIPES
contactez-nous à annonces@village-justice.com

www.village-justice.com

legiteam Editions

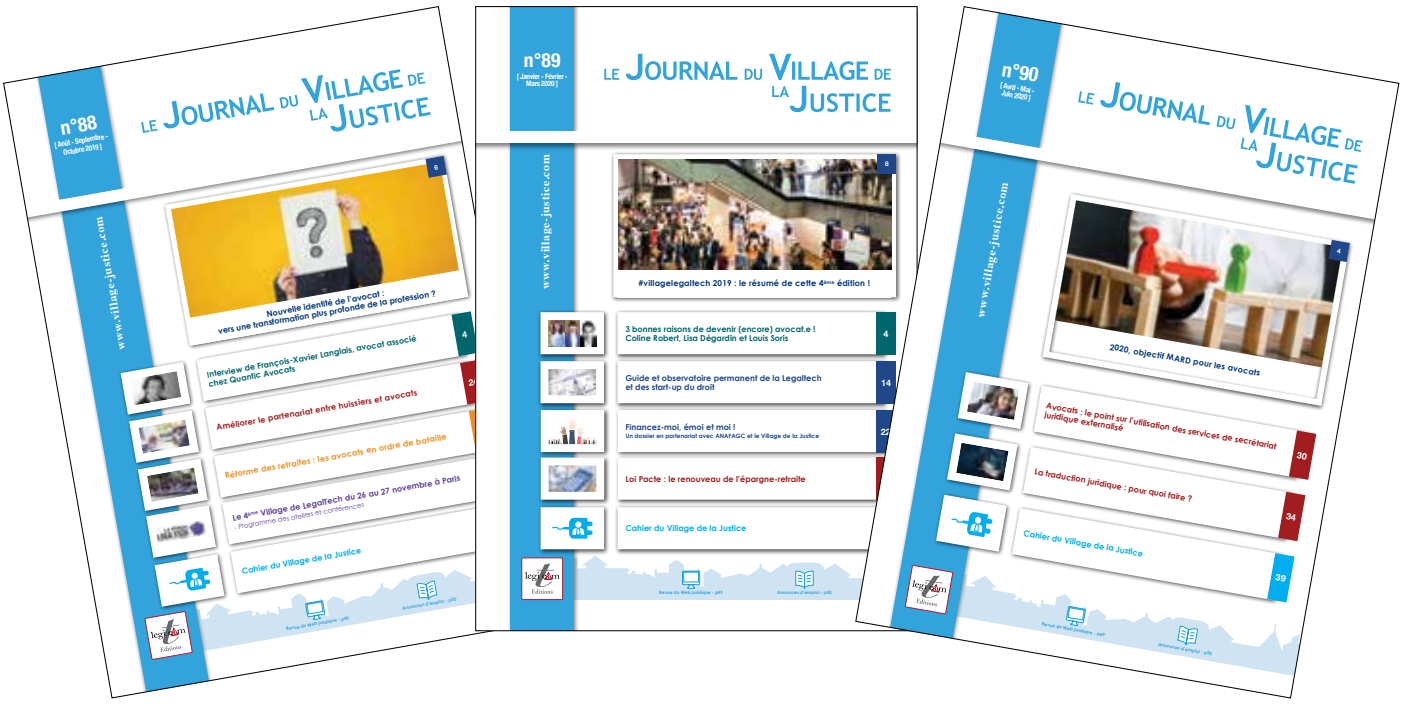
LEGI TEAM

04 76 16 82 50 ou 01 70 71 53 80
annonces@village-justice.com
www.legiteam.fr

* Source : ACPM moyenne fin 2019

Vous êtes à la recherche de réponses sur le management de votre cabinet

Abonnez-vous gratuitement au Journal du Village de la Justice



1er journal dédié au management d'un cabinet d'avocats :

vous y trouverez des dossiers pratiques, l'actualité de la profession, des offres d'emploi, l'agenda juridique...

Cabinet : .....
Madame / Monsieur : .....
Prénom : .....
Nom : .....
Adresse : .....
Code Postal : .....
Ville : .....
E-mail : .....
Téléphone : .....

Abonnement gratuit au Journal du Village de la Justice

« Conformément à la loi Informatique et libertés du 6 janvier 1978, vous disposez d'un droit d'accès, de rectification et d'opposition aux données personnelles vous concernant. Pour mettre en œuvre ce droit, il vous suffit de nous contacter en nous précisant vos nom, prénom, adresse, e-mail : par e-mail à legiteam@legiteam.fr par courrier à LEGI TEAM, 198 avenue de Verdun 92130 Issy-les-Moulineaux »

Cahier du Village de la Justice

réalisé par www.village-justice.com

SOMMAIRE

LES AVOCATS SE CACHENT POUR MOURIR !

Non, c'est une boutade, du moins espérons-le. Les avocats ne se cachent pas pour mourir mais tentent de survivre. Certains réussissent d'ailleurs relativement bien. D'autres non. Pour diverses raisons que les rapports successifs sur la profession, très hétérogène, expliquent. En revanche, du moins en France, les risques psychosociaux ne semblent pas mobiliser. Ils contribuent pourtant à fragiliser la profession qui a l'art du camouflage. D'où l'écriture d'un Guide sur les Risques Psychosociaux des Avocats (Première édition). Les tabous sont faits pour être levés.

La couleur de la robe est le même que celle du deuil. Pourtant la profession d'avocat n'est pas prête à rendre l'âme. Malgré les grèves plus paralysantes qu'efficaces, les deux confinements, les réformes incessantes donnant le tournis, les enjeux de cette profession universelle, si résiliente que cela en devient inquiétant, détonnent.

Pour cela, la santé mentale et physique des praticiens reste évidemment une priorité. En théorie. Car, contrairement aux médecins qui tirent la sonnette d'alarme, bardés d'un nombre impressionnant d'enquêtes et de sondages sur leurs souffrances, les avocats, eux, aux allures de Samouraïs, cultivent, en apparence, résistance et endurance. Les praticiens du droit souffrent en silence et se cachent peut-être même pour mourir. Qui sait, la profession si diverse pourrait ne pas avoir vraiment d'unité.

Quelques enseignements sur les risques psychosociaux existent bien, çà et là. Mais fondamentalement, l'avocat qu'on promet augmenté, digital, numérique, as de l'intelligence artificielle, qui en montrera, s'avère en péril.

En France, nous n'avons pas de spécialistes des risques psychosociaux des avocats comme la professeure canadienne Nathalie Cadieux ou l'avocat californien Patrick Krill. A quoi bon, les colloques annoncés de toute part donnent le change, La profession innove, est à la pointe, demeure un partenaire ou un adversaire sans faille du gouvernement, qu'elle défie, tente de convaincre, résiste, propose. Elle a raison.

Mais l'avocat ressemble à un polytraumatisé, muet de douleur, refusant les soins qui finissent par devenir palliatifs. Donner le change à travers un déni au lieu d'opter pour le vrai changement ? Tant que le pied du miroir tient, le reflet ne tremble pas.

Les syndicats s'essaient régulièrement à la démonstration. Mais l'interdépendance des avocats, magistrats, greffiers, qui justifierait un syndicat unifié pour lutter contre les RPS, est encore un concept préhistorique. Churchilliens, les représentants de la profession sont des modèles d'abnégation. Sans être capables d'unir.

Parlons un peu du Guide des Risques Psychosociaux des Avocats.

Le guide est divisé en 42 chapitres. On ne peut plus et mieux verser dans la simplicité. Les sources très riches à la fin de chacun d'eux. Les traquer n'est pas aisé. Elles sont le plus souvent en anglais, dispersées, multiples. L'entreprise d'écrire un tel guide est une cavalcade mais pas à bride abattue. Il a fallu sélectionner d'une manière draconienne les thèmes. Pas une thèse. Pas un rapport. Ce guide contient juste des pistes, pour justement éviter le hors piste et l'avalanche. L'appel de phare dans les

yeux. Sans chercher à éblouir, juste à réveiller, pour, à terme, éveiller. Un essai, cette première édition, car elle se complétera très vite en une deuxième fournée et détonnera. Le Guide recense des exemples de RPS et leur traitement dans d'autres pays que la France, pour comparer, mettre en perspective.

D'abord, l'hommage à la professeure Nathalie Cadieux et à ses si courageux équipiers, dont Martine Gingues. Une équipe de choc. Une task force. Des études sur l'ensemble des RPS des avocats, dont les addictions, sous l'égide du Barreau de Montréal, sur la durée, complètes, nourries, documentées, qui font autorité. Une référence incontournable, la professeure Cadieux, de Sherbrooke. Mais dont on ne parle pas en France.

Le Pamba, le service d'aide du Barreau de Montréal, ressemblerait à s'y méprendre à un hôpital virtuel pour avocats.

Enchaînement sur les actions de l'association du Barreau du Canada, du Barreau de Paris, du Royaume-Uni, des Barreaux américains.

Palme d'or pour l'avocat californien Patrick Krill, spécialiste des RPS de la profession. Une gigantesque étude est en cours portant sur 70 000 professionnels.

Du Krill, associé à un professeur de psychiatrie, surpuissant, pionnier, déjà très remarqué pour ses travaux sur la question. Lecture conseillée de mon article sur ce même site, sur les questions portant sur la santé mentale des candidats aux Barreaux américains.

Et puis, on arrive à un triste constat. La sirène du Stuka en piqué. Nos jeunes. Les étudiants en droit. Faculté. Ecoles d'avocats. Comment les traite-t-on en France ? On ne les maltraite même pas, on fait comme si ils n'existaient pas. On ignore la prévention.

On rentre enfin dans le vif. Certaines pathologies. Le burn out. Le séisme. La dépression. Deux maladies invalidantes, destructrices, traîtres, venant sur la pointe des pieds, évoluant à bas bruit.

D'autres affres guettent la profession. Le stress, l'aigu, le post traumatique.

L'extrême, les suicides des avocats. Aucune étude en France. Les psychiatres français ne s'intéressent pas aux avocats et les avocats ne s'intéressent pas aux avocats. Ces derniers ont l'art du camouflage et le divorce avec la médecine est un fait.

Cerner les RPS des avocats, c'est ne jamais oublier les clients. Faire face à leurs failles psychologiques, fait partie du job. Mais quand un client met fin à ses jours, l'onde de choc n'est pas un effet optique. L'avocat doit apprendre à se protéger.

Dans e passé, en France, la guillotine. L'enfer. Assister à l'exécution de son client. Coutume ? Etait-ce nécessaire ? Il faut lire l'Abolition de Badinter. Le bruit de la lame. Le sang. Le panier. L'avocat français n'est plus concerné.

Actuellement, ailleurs, notamment aux States, toujours, la dose létale, la chaise électrique, le peloton d'exécution, la pendaison.

Brow out, *blur out*, locutions anglophones aux faux airs branchés mais redoutables.

Puis on attaque un gigantesque chapitre qui restera comme les autres tout petit, dimension du guide oblige. Le sommeil. Causes et conséquences des RPS. Son architecture mérite d'être connue.

Ensuite, le combat poignant des avocats souffrant de handicaps, visibles ou invisibles et le travail de deux associations pionnières, Droit Pluriel et Droit comme un H, pour leur recrutement et leur intégration.

La profession en France est familière de l'omerta dans certains domaines. Harcèlement de tout ordre, racisme, discriminations, exclusion. Le rapport de Jacques Toubon, Défenseur des droits, a été d'ailleurs une véritable bombe atomique. Pensez-vous, la profession d'avocat qui se fait rappeler sa vocation, défendre les plus faibles, notamment les siens. Rappel des actions du Barreau de Paris.

Mais le versant parisien ne vaut pas le versant canadien. Brad Regehr, originaire des Premières Nations canadiennes, vient d'être élu président des 37 000 avocats de l'association du barreau canadien. Vous lirez mon article publié sur ce même site, sur la diversité ethnoculturelle dans la justice canadienne. L'association du barreau autochtone mène aussi une lutte âpre et sans merci contre la discrimination au Canada.

En France, nous ne savons pas combien d'avocats de couleur noire exercent. Poser la question revient à poser un problème. Au Canada, l'initiative *BlackNorth* pulvérise les habitudes, celles de proclamer des principes au lieu d'agir. *BlackNorth* un engagement à éradiquer le racisme systémique. Les plus grands avocats canadiens y souscrivent. Tout est fait, nous lirons les lettres du 14 septembre 2020 adressées au pouvoir exécutif, pour exhorter le gouvernement à nommer des personnes autochtones, noires et de couleur (PANDC) dans la magistrature canadienne. Le débat est ouvert, à vif, sans limite relancé par Brad Regehr, succédant à Vivene Salmon, ex présidente de couleur noire.

Toutefois, l'avocat est bien souvent en sursis. Assassinat par la pègre, les mafias, les cartels. Menaces de groupes terroristes. Les persécutions politiques font plus que jamais de l'avocat une cible, lui et ses proches. Les pires RPS en découlent. De Nelson Mandela à un nombre astronomique

d'avocats emprisonnés et torturés en Chine, à Hong Kong, en Turquie, en Iran. Que faire ? Exemples dans le guide.

Un aspect oublié, les RPS inhérents à l'exposition médiatique. Le craving de la célébrité éphémère et la chute libre. Savoir s'entourer.

Puis, les RPS découlant de l'image publique de la profession. Les pilleurs de CARPA, les blanchisseurs d'argent sale font beaucoup de mal à la profession. Les conflits de valeur pullulent et poussent au départ de la profession. Fantastique réussite du consortium des journalistes indépendants, que d'avoir mis à jour les *Panamas Papers*.

Autre énorme risque dans la vie de l'avocat, le *hacking*.

Doxing oblige, attention aux publications sur Internet.

Les troubles musculo-squelettiques font des ravages, que probablement une meilleure utilisation des documents uniques d'évaluation des risques professionnels pourrait amoindrir.
Parler du confort "corporel" de l'avocat revient à aborder la typologie de son bureau. Comment le télétravail peut-il tout remettre en question. L'avocat sera-t-il encore plus nomade en ces temps covidiens ?

Parmi beaucoup d'autres thèmes, quelques réflexions sur les déplacements de l'avocat, l'annonce au client d'un échec, le *coping*, le travail le week-end, quand le juge est un inconnu, la nécessité de savoir refuser un dossier.

Sans oublier le bouleversement provoqué par la Covid-19 avec les multiples mésaventures lors du passage de certains examens d'avocats en ligne, aux Etats-Unis et au Canada.

Alors, face à tant de RPS aussi divers, quelles parades ? Les groupes Balint, comme celui du Barreau de Paris, le mentorat, le *counselling*, le yoga, la méditation, le repérage, sont des pistes très efficaces. Aura-t-on un jour des salles de yoga et de méditation parfaitement ventilées, communes aux avocats, magistrats, greffiers au sein des tribunaux ?

Dernier chapitre du guide mais dont le thème, la reconversion, est si important.

Rebondir.

Les conséquences des RPS non maîtrisés aboutissent fréquemment à une reconversion désirée, préparée ou imposée. Là aussi, les capacités de mobilité professionnelle de l'avocat sont perfectibles. Beaucoup de praticiens rêvent de faire autre chose mais procrastinent. L'avocat reconverti n'est pas un repenti. Il revient bien souvent au Barreau plus fort, dans une niche, doté d'un réseau. Exemples et conseils. Les Nostradamus de la profession, les éditeurs de logiciels, les start up, les legal tech continueront de dessiner des plans sur la comète et de spéculer, tant sur les nouveaux rôles de l'avocat que sur ses modalités de travail. C'est d'ailleurs très bien. Mais en oubliant, régulièrement, que les neurosciences n'abstraient pas les fonctions du cerveau mais en découlent, sans toutefois le contrôler. Il est de toute façon bien téméraire de dresser le portrait de l'avocat de demain, tellement il devra s'adapter et répondre aux besoins d'une clientèle très hétérogène.

Une chose est certaine, une santé préservée lui permettrait évidemment d'affronter certaines transitions. La prise de conscience et les actions de prévention des RPS sont parfaitement possibles, sans délai.

Si la volonté est présente.

Sinon, désastre annoncé.

A suivre.

Vincent Ricouleau

Auteur du Guide sur les risques psychosociaux des avocats

Professeur de droit -Vietnam -
Directeur fondateur de la clinique francophone du droit au Vietnam

Titulaire du CAPA - Expert en formation pour Avocats Sans Frontières -

Titulaire du DU de Psychiatrie (Paris 5), du DU de Traumatismes Crâniens des enfants et des adolescents (Paris 6), du DU d'évaluation des traumatisés crâniens, (Versailles) et du DU de prise en charge des urgences médico-chirurgicales (Paris 5).

AVOCATS : QUELQUES CONSEILS POUR PRÉSERVER VOTRE ÉQUILIBRE DE VIE.

Un bon équilibre entre vie professionnelle et vie privée est essentiel pour un avocat, tant sur le plan professionnel que personnel. Pour réussir à long terme, vous devez avoir le bon équilibre entre votre pratique du droit et votre vie personnelle. Trop de travail au sein de votre cabinet en vous sacrifiant en tant que personne, est contre-productif.

Vous connaissez probablement un avocat tellement concentré sur sa carrière, que sa vie en dehors du travail, son conjoint et ses enfants en ont été victimes. Le divorce et l'éloignement de ses enfants en sont souvent les résultats : vous êtes plus que des avocats, plus que ce que vous faites dans la vie.

Pour qu'un avocat réussisse, il doit être accessible par ses clients à tout moment, n'est-ce pas ?

Faux. Certes, il est important d'être disponible pour les clients, mais cela doit être une disponibilité raisonnable. Dans notre environnement moderne, vous ressentez parfois la pression d'être disponible 24 heures sur 24, 7 jours sur 7. Le piège est que si vous êtes trop disponible, vos clients s'y attendront. Et, la plupart du temps pour la plupart de vos clients, ce n'est tout simplement pas nécessaire. Bien sûr, si vous êtes au milieu d'une transaction aux enjeux élevés ou si vous vous préparez pour un jugement qui aura lieu un lundi, vous devrez peut-être être accessible. Mais sinon, votre client peut généralement attendre votre présence au cabinet.

Vous devez former vos clients à travailler en fonction de vos horaires de travail.

Prenons l'hypothèse que vous souhaitiez parler à votre médecin. Vous appelez son bureau et sa secrétaire vous dit que le médecin retourne les appels entre 16 h et 17 h. Ce n'est généralement pas un problème, n'est-ce pas ? Vous comprenez qu'il est occupé et sachant que vous recevrez un rappel à un moment donné, vous pouvez planifier votre disponibilité. Alors pourquoi ne pouvez-vous pas faire la même chose dans votre pratique du droit ?

De nombreux avocats sont fréquemment au tribunal le matin. Leurs clients ont été formés pour ne pas s'attendre à ce qu'ils soient disponibles le matin afin qu'ils n'appellent pas à ce moment-là.

Le même principe s'applique à votre temps personnel.

Pour un bon équilibre entre vie professionnelle et vie privée, il doit y avoir des moments où vous n'êtes pas à l'écoute des clients. Il y a plusieurs façons de faire ça.

Une façon est de ne pas donner votre numéro de téléphone mobile ou domicile. Si nécessaire, informez vos clients que vous vérifierez vos messages pendant le week-end.

Une autre façon est de donner aux clients votre numéro de portable mais en posant des limites. Faites-leur savoir que vous êtes là pour eux en cas d'urgence et, en cas d'urgence seulement, ils peuvent vous appeler à ce numéro pendant le week-end ou après les heures de présence au cabinet. En le présentant de cette manière, vous aurez relevé le seuil de ce qu'est un appel acceptable. La plupart des clients, ceux que vous voulez de toute façon, respecteront cela.

L'email est une autre intrusion dans le temps personnel. Vous pouvez former vos clients en leur faisant savoir que vous ne lisez pas vos emails après les heures d'ouverture du cabinet ou le week-end. S'ils comprennent que vous ne les lisez pas, il leur sera difficile de s'énerver lorsque vous ne répondez pas à leur email.

Si cela vous semble un peu difficile, essayez de dire à vos clients que vous ne vérifiez pas vos emails durant votre temps libre, mais qu'en cas d'urgence, ils peuvent appeler votre téléphone portable. Une fois encore, vous avez relevé le niveau d'acceptation et formé votre client d'une manière efficace afin qu'il ne vous dérange pas durant votre temps libre à moins que ce ne soit extrêmement important.

Trouver l'équilibre entre votre pratique du droit et votre vie personnelle est un défi permanent, mais qui mérite des efforts continus. Posez des limites. C'est votre vie, cela en vaut la peine.

Joël Jégo
joeljego@activetransition.net
https://activetransition.net/coaching-avocats/

REVUE DU WEB JURIDIQUE

A lire sur le Village de la Justice en ce moment...

(Vous pouvez saisir l'adresse complète pour consulter l'article, ou « flasher » le code 2D pour y accéder directement depuis votre Smartphone. Logiciel gratuit à télécharger à mobiletag.com)

Observatoire de l'interprofessionnalité des métiers du droit.

L'interprofessionnalité est l'un des axes forts de la transformation des métiers du droit. Elle a connu un renouveau suite aux ordonnances Macron de 2016 et la création notamment des S.P.E (Société Pluriprofessionnelle d'Exercice), l'une des modalités de cette nouvelle forme de collaboration entre les professions. Elle répond à une demande exprimée par la clientèle et s'inscrit dans une tendance croissante à vouloir exercer différemment, à l'image des réflexions autour des coopératives. Le Village de la justice vous propose ici un annuaire mis à jour régulièrement et recensant les structures interprofessionnelles existantes, à la fois pour s'informer de l'état du « marché » et - pourquoi pas -trouver inspiration et conseils auprès de ceux qui se sont lancés.

En savoir plus sur
http://www.village-justice.com/articles/flashcode,36622.html

2020, l'année des protections juridiques ?

Le secteur des protections juridiques suit un chemin discret. Une discrétion paradoxale au vu de la croissance que connaissent ces assurances. Elles n'hésitent pas désormais à s'appuyer sur toutes les solutions innovantes du marché du droit. Hubert Allemand, Président du Groupement des Sociétés de Protection Juridique, analyse pour le Village de la Justice le présent et l'avenir de ce marché.

En savoir plus sur
http://www.village-justice.com/articles/flashcode,36993.html

Pourquoi la crise du coronavirus doit être un accélérateur pour l'usage des technologies dans les métiers du droit.

Jusqu'ici, les parties prenantes étaient plutôt figées dans des postures un peu monolithiques. D'un côté, les partisans de la techno "quoi qu'il arrive", de l'autre, ceux clamant que l'intelligence artificielle allait détruire leur métier. Entre les deux, "le ventre mou décisionnel", figé dans une position d'attente de clarification. Et les débats se sont prolongés pour ou contre la techno pour améliorer le droit.
Mais la période Covid-19 est venue d'un seul coup déplacer le débat sur des enjeux plus immédiats et opérationnels, la mobilité, la flexibilité, la collaboration à distance et le maintien du service du droit. On parle d'autres aspects des technologies, et c'est tant mieux...

En savoir plus sur
http://www.village-justice.com/articles/flashcode, 35781.html

Avocats, comment communiquer sur les réseaux sociaux ?

Créer un profil sur les réseaux sociaux, c'est à la portée de tous. Ce qui l'est moins, c'est de faire vivre correctement ce profil qui doit refléter au plus près votre personnalité professionnelle et votre activité, vous mettre en avant sans être pour autant une mise en scène narcissique, le tout en respectant les règles déontologiques de la profession. Un exercice de funambule donc. Voici les conseils des experts.

En savoir plus sur
http://www.village-justice.com/articles/flashcode,36761.html

[Enquête] Assistant.e.s et secrétaires juridiques : comment vont-elles/ils ?

Il était grand temps de prendre de nouveau la température de la profession de secrétaire juridique, et elles/ils sont 135 à s'être confié.e.s au travers de nos questions et des commentaires que nous leur avions proposé de faire.
Voici les résultats de cette nouvelle enquête qui en dit long sur une profession visiblement sous pression, et qui demande (ce qu'elle faisait déjà il y a une décennie en arrière) plus de reconnaissance professionnelle et salariale…

En savoir plus sur
http://www.village-justice.com/articles/flashcode,36768.html

Chroniqueur judiciaire, ou l'art de transporter les citoyens dans la salle d'audience.

"Historique" : c'est ainsi que le procès des attentats de janvier 2015 contre le journal Charlie Hebdo et l'Hyper Cacher a été qualifié, en raison notamment de la charge émotionnelle individuelle et collective qu'il porte, mais aussi du fait qu'il soit filmé en vue de la constitution d'archives de la justice.
Un procès hors norme donc qui nécessite un suivi qui l'est tout autant et qui vient mettre en lumière un travail journalistique particulier, celui de chroniqueur judiciaire.
Charlotte Piret, qui officie en tant que chroniqueuse judiciaire sur France Inter, nous raconte l'âme de son métier au travers du suivi de ce procès qui est entrain de s'inscrire dans l'Histoire française.

En savoir plus sur
http://www.village-justice.com/articles/flashcode,36658,html

Vous aussi, auto-publiez-vous et bénéficiez d'équivalence formation !

Le Village de la Justice, 1er site de la communauté des professions du droit avec 1 800 000 visites par mois, vous propose de vous auto-publier. Publiez sur notre site (rubrique Blog) un article, qui une fois validé par notre rédaction, sera consultable par toute la communauté, mais aussi par l'ensemble des internautes (après mise en ligne, votre article sera référencé notamment par Google en quelques minutes).

OFFRES D'EMPLOIS

Voici une sélection d'annonces en cabinets d'avocats.
Retrouvez ces annonces et bien d'autres chaque jour, sur toute la France, sur www.village-justice.com/annonces

AVOCAT (H/F) POLYVALENT - PARIS / BLANC-MESNIL / AULNAY SOUS BOIS - CABINET JS

Spécialités : Droit des affaires et des étrangers

Notre cabinet, composé de 9 juristes, intervient dans le cadre du droit aux étrangers et le droit des affaires.
Dans le cadre de l'expansion de son activité en pleine expansion, le cabinet JS recherche un(e) avocat(e) (H/F) capable de traiter des dossiers liés au droit des affaires et le droit aux étrangers.

La collaboration se fera dans un cadre négocié selon le profil du (de la) candidat(e).

L'âge ne rentre pas en ligne de compte, mais les candidatures de jeunes avocats sont aussi souhaitées. (peu d'expérience acceptée)

Profil :
• Dynamique, maitrisant les outils informatiques, disponible, ayant un goût pour le challenge et le défi, mobile
• Parler plusieurs langues serait un plus.
• Une formation au droit des étrangers pourra être donnée pour ceux et celles qui ne sont pas encore rompus à cet exercice.
• La connaissance du droit des affaires est requise.

Merci de postuler par email à current@cabinetjs.com

COLLABORATION 3/5 ANS DROIT SOCIAL (H/F) – PARIS - TEILEN AVOCATS

Spécialités : Droit du travail : relations individuelles et collectives

Cabinet d'avocats spécialisé en droit du travail recherche un(e) collaborateur(trice) ayant 3 à 5 ans de barreau avec une expérience réussie en cabinet d'avocats spécialisé en droit du travail.

Vous interviendrez en conseil (relations collectives et individuelles) et en contentieux auprès d'une clientèle d'entreprises, groupes français et étrangers de toutes tailles et tous secteurs d'activités, ainsi que de cadres.
Vous travaillerez avec les deux associées du Cabinet qui sont très attachées à la cohésion d'équipe et à l'échange des idées.
Le Cabinet favorise l'évolution des compétences des collaborateurs et tient à l'équilibre entre vie professionnelle et vie privée ce qui passe notamment par la possibilité de télétravail.

Titulaire du CAPA, ayant de préférence un 3ème cycle en droit social (Master II, DJCE...) ou une solide expérience en entreprise.

Rigueur, travail en équipe, capacité à confronter ses idées sont des qualités attendues du candidat.

Merci de postuler par email à gteissedre@teilenavocats.fr

COLLABORATION LIBÉRALE DROIT SOCIAL (H/F) - PARIS 75116 PORTE DAUPHINE - ON AVOCATS

Spécialité : Droit du travail

Le cabinet ON AVOCATS, spécialisé en droit des affaires (fiscal, corporate, commercial et social), basé porte Dauphine à Paris (75116), recherche un Avocat Collaborateur Libéral Confirmé (H/F) pour renforcer son équipe en droit social :

Missions :
Vous interviendrez dans des missions de conseil (relations individuelles et collectives) et contentieux auprès d'une clientèle d'employeurs de secteurs économiques variés.

Profil :
Titulaire d'un Master 2 en Droit Social et du CAPA, vous avez acquis une expérience d'au moins 2 ans dans un cabinet reconnu pour sa pratique en droit social.

Vous aimez travailler en équipe, vous êtes motivé et dynamique.
Vous avez de bonnes connaissances juridiques et de mise en pratique, permettant d'apporter une vraie valeur ajoutée aux clients, vous possédez un esprit d'analyse, de synthèse et de rigueur avec d'excellentes qualités rédactionnelles.
Vous avez une bonne maitrise des outils bureautiques et digitaux.

Merci de postuler par email à svial@onavocats.com

COLLABORATEUR EN DROIT SOCIAL (H/F) - PARIS 16 - AKLEA, SOCIÉTÉ D'AVOCATS

Spécialité : Droit social

Aklea, société d'avocats est un cabinet d'avocats français indépendant qui regroupe plus de 50 personnes dont 9 associés sur deux sites en France, Paris et Lyon.
Aklea recherche pour son bureau de Paris Un(e) Avocat(e) collaborateur spécialisé(e) en Droit social

Vos missions :
Dans le cadre de notre ligne de services « Social, ressources humaines et mobilité internationale », vous accompagnerez nos clients français et étrangers.
Vous interviendrez principalement dans le domaine du conseil, tant sur le plan des relations individuelles (rédaction de contrat de travail, procédure de licenciement...) que collectives (négociation et rédaction d'accords d'entreprise, élaboration de PSE...).
Vous assisterez la clientèle devant les juridictions de droit du travail et de la sécurité sociale

Votre formation :
Titulaire du CAPA et ayant d'un 3ème cycle en droit social (Master II, DJCE...) ;
De 2 à 3 ans de barreau avec une expérience réussie au sein de cabinets d'avocats spécialisés en droit social ;
Une maîtrise de l'anglais courant et juridique est indispensable.

Vos qualités :
Vous êtes rigoureux (se), autonome, avez le sens du travail en équipe et faites preuve de rapidité d'analyse ;
Vous aurez à cœur d'accompagner le développement de la ligne de services.

Merci de postuler par email à recrutement@aklea.fr

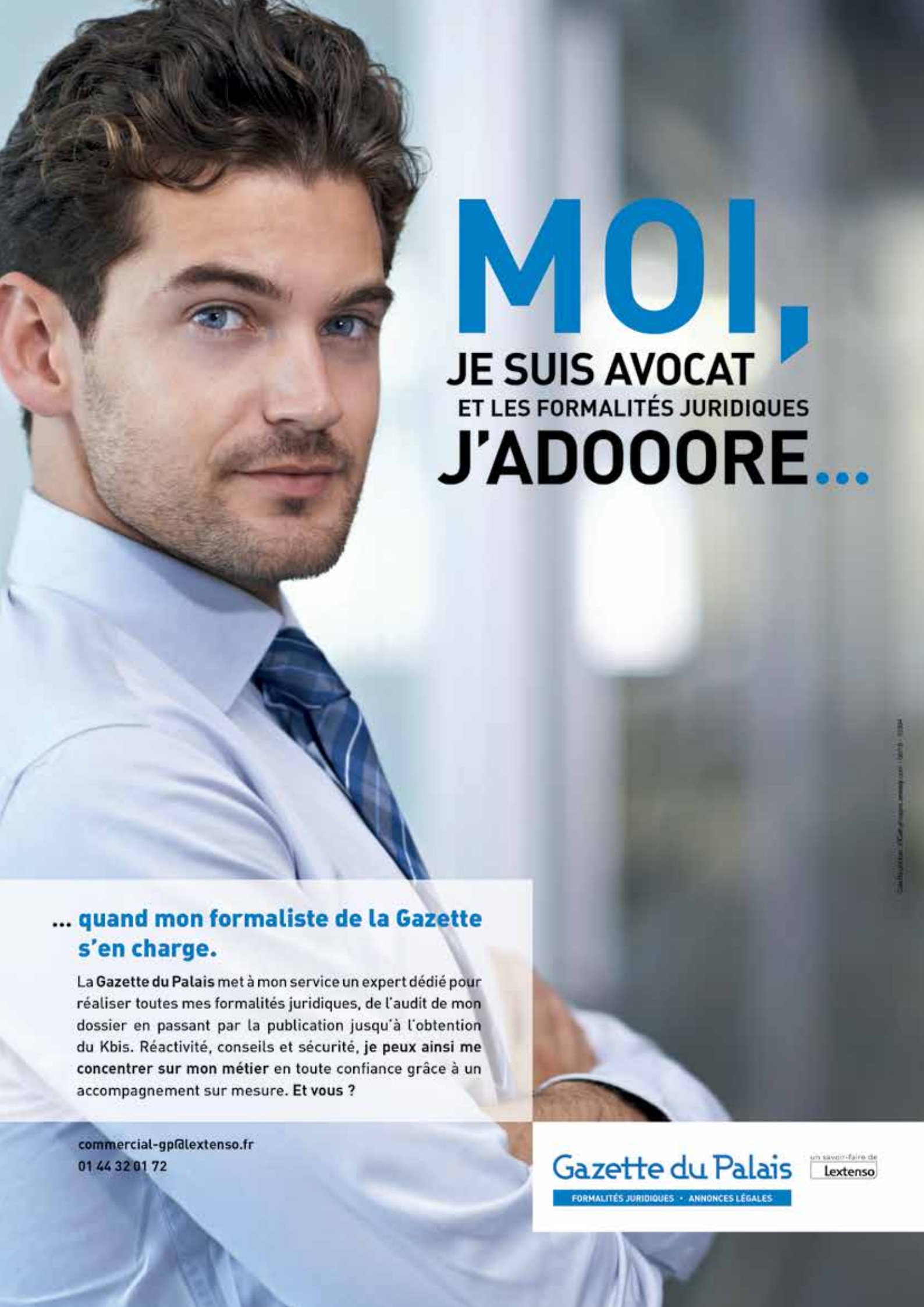
POSTE DE COLLABORATEUR(TRICE) LIBÉRAL(E) EN DROIT DE LA FAMILLE - PARIS (16ÈME) - CABINET FAMILYNKS AVOCATS

Spécialités : Droit de la famille, des personnes et de leur patrimoine

Cabinet Familynks dédié au droit de la famille interne et international, recherche un(e) collaborateur(trice) afin de compléter son équipe composée de deux associés, d'une collaboratrice et d'une stagiaire.
Vous disposez d'un Master II de droit privé/droit de la famille et vous avez d'ores et déjà une expérience au minimum de deux années dans un cabinet spécialisé en droit de la famille.
Nous recherchons des candidats disposant de qualités rédactionnelles et d'écoute, d'un bon esprit de synthèse et désireux de s'investir au sein d'un cabinet en développement.

Le poste est à pourvoir à compter du mois de janvier 2021.

Nous vous invitons à consulter notre site internet www.familynks.fr et adresser vos CV et lettres de motivation par mail en postulant à contact@familynks.fr



... quand mon formaliste de la Gazette s'en charge.

La **Gazette du Palais** met à mon service un expert dédié pour réaliser toutes mes formalités juridiques, de l'audit de mon dossier en passant par la publication jusqu'à l'obtention du Kbis. Réactivité, conseils et sécurité, **je peux ainsi me concentrer sur mon métier** en toute confiance grâce à un accompagnement sur mesure. **Et vous ?**

commercial-gp@lextenso.fr
01 44 32 01 72

Gazette du Palais
FORMALITÉS JURIDIQUES · ANNONCES LÉGALES

un savoir-faire de Lextenso

www.transformations-droit.com

#transfodroit

Le Village de la LegalTech se transforme et devient

les rendez-vous
TRANSFORMATIONS du DROIT

11/12 mars 2021 | PARIS

Pour vous accompagner dans votre transformation, Open Law*, le droit ouvert et le Village de la Justice vous donnent rendez-vous sur les 5 Villages du Salon.

VILLAGE DE LA LEGALTECH
aux RDV « TRANSFORMATIONS DU DROIT »
11/12 mars 2021 | PARIS

VILLAGE DU LEGAL DESIGN
aux RDV « TRANSFORMATIONS DU DROIT »
11/12 mars 2021 | PARIS

VILLAGE DES TRAJECTOIRES PROFESSIONNELLES
aux RDV « TRANSFORMATIONS DU DROIT »
11/12 mars 2021 | PARIS

VILLAGE DES INNOVATEURS PUBLICS
aux RDV « TRANSFORMATIONS DU DROIT »
11/12 mars 2021 | PARIS

VILLAGE DE LA REGTECH
en 2020 avec Le Cercle Montesquieu
aux RDV « TRANSFORMATIONS DU DROIT »
11/12 mars 2021 | PARIS

Un événement organisé par

OPEN LAW*
*Le droit ouvert

VILLAGE DE LA JUSTICE
La communauté des métiers du droit
BY LEGI TEAM