ORDRE DES AVOCATS DE PARIS

VADE MECUM DE LA DEONTOLOGIE DU NUMERIQUE

Les FAQ de l'Ordre des avocats au barreau de Paris

Décembre 2013

VADE MECUM DE LA DEONTOLOGIE DU NUMERIQUE

Ce guide est constitué d'une série de recommandations et de FAQ[1] qui répondent à la plupart des questions que peuvent se poser les avocats lorsqu'ils créent leur site internet, ouvrent leur profil sur un réseau social professionnel ou font appel à des prestataires extérieurs, en externalisant certaines fonctions de leur cabinet.

Elaboré par les Membre du Conseil de l'Ordre en charge des commissions de déontologie, il a pour objectif de répondre de façon simple et pratique aux questions les plus fréquentes que se posent les avocats en matière de déontologie dans le domaine des technologies du numérique.

Si le croisement des nouvelles technologies et de la déontologie peut apparaître comme délicat, il convient d'avoir à l'esprit un principe simple : L'avocat est en toutes circonstances tenu de respecter les règles déontologiques. En d'autres termes, l'évolution de notre exercice professionnel induit par les nouvelles technologies que chaque avocat met en œuvre dans son cabinet ne peut l'affranchir, non seulement du respect des dispositions du règlement intérieur national (RIN) et du règlement intérieur du barreau de paris (RIBP), mais de l'obligation de faire respecter ces règles par l'ensemble des membres de son cabinet et par les prestataires extérieurs auxquels il fait appel pour les besoins de son activité.

Cette règle impérative concerne aussi bien l'externalisation de certains services du cabinet (standard déporté, secrétariat à distance, traducteur, etc.) que l'externalisation des données du cabinet (Cloud Computing) et la mise en œuvre de ses outils de communication (site Web, blog, sites de référencement, site tiers, consultation en ligne, etc.). 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.

Christophe Thévenet
Membre du Conseil de l'Ordre

Décembre 2013

[1] ***FAQ*** *: Une* ***foire aux questions****, par rétro acronymie à partir de l'acronyme anglais* ***FAQ*** *pour frequently asked questions (littéralement « questions fréquemment posées »), est une liste faisant la synthèse des questions posées de manière récurrente sur un sujet donné, accompagnées des réponses correspondantes, que l'on rédige afin d'éviter que les mêmes questions soient toujours reposées, et d'avoir à y répondre constamment (Source : Wikipedia).*

Les thèmes abordés dans le présent guide sont les suivants :

1. la sécurisation des données du cabinet :

- Sécurisation physique des ordinateurs et des devices : téléphone, PDA, tablettes
- La sécurité de l'informatique du cabinet : firewall, accès à distance
- Sauvegarde des données

2. Les fonctions externalisées :

- Garanties à obtenir du prestataire externe : secrétariat, standard, traducteur, expert, etc.
- L'externalisation des données du cabinet (cloud computing)

3. Le site web du cabinet

- Contenu
- Les mentions légales
- Procédure de validation par l'ordre
- Les blogs

4. Les réseaux sociaux

5. Le référencement

6. L'intermédiation : l'utilisation de site tiers pour développer sa clientèle

Ont contribué à la rédaction du présent guide :

Membres du Conseil de l'Ordre :

Monsieur Thomas Baudesson
Secrétaire de la commission de déontologie *« Secret professionnel et confidentialité »*
Monsieur Alexandre Moustardier
Secrétaire de la commission de déontologie « *Publicité, démarchage et communication* »
Monsieur Vincent Ohannessian
Secrétaire de la commission de déontologie « *Respect du contradictoire* »
Monsieur Dominique Piau
Secrétaire de la commission de déontologie « *Ducroire* »
Monsieur Christophe Thévenet
Secrétaire des commissions ordinales de déontologie

Ancien membre du Conseil de l'Ordre :

Madame Sarah Baruk,
Membre de la commission de déontologie « *Publicité, démarchage et communication* »

1. Sécurité informatique du cabinet[2] et sauvegarde des données : la base

1.1. Comment protéger physiquement les appareils stockant les données ?

La sophistication croissante des moyens de protection de nos données informatiques ne doit pas nous faire perdre quelques règles de bon sens :

- Les **ordinateurs** : attacher les portables (notebooks) par un **câble de sécurité** à son bureau pour éviter le vol (c'est possible également avec un desktop même si le « vol d'opportunité » est moins probable ; sinon, fermer son bureau à clé en cas d'absence ; les garder près de soi en déplacement (éviter de les laisser dans un bagage en soute en avion ou dans l'espace commun bagages en train) ;

- Les **disques durs externes et autres clés usb** : les mettre sous clé (tiroir, armoire….)

- **Les devices (téléphones, PDA, tablettes)** : encore plus exposés au vol ou à la perte, ces appareils doivent être protégés physiquement, tout simplement en les conservant avec soi. Ils devront également être protégés par mot de passe (distinct de la clé « PIN ») : à défaut toute personne entrant en possession de votre PDA pourra consulter vos mails et les pièces jointes, c'est-à-dire l'ensemble des données de vos clients.

1.2. Comment protéger logiquement vos ordinateurs

- **Toujours mettre un mot de passe sur son ordinateur**, non seulement pour l'ouverture d'une session mais également en activant **l'écran de veille** avec « réveil avec mot de passe » : on peut configurer par exemple le temps de mise en veille à 5 mn ce qui permet d'éviter l'accès à son ordinateur (et donc, potentiellement, la copie de données) lorsque l'on quitte son bureau temporairement (pour déjeuner ou partir en rendez-vous par exemple). Sur les disques durs externes portables, il est également possible d'instaurer un mot de passe pour accès réservé ;

- **Eviter de laisser son ordinateur allumé** lorsque l'on quitte le cabinet ou que l'on arrête de l'utiliser ;

- **Installer obligatoirement un logiciel antivirus/sécurité Internet sur son ordinateur** : ce logiciel doit a minima pouvoir analyser l'ensemble des fichiers présents sur l'ordinateur ou ses périphériques, permettre l'analyse des emails entrants et de leurs pièces jointes, comporter une surveillance Internet avec, notamment, un firewall configurable. Le faire même si le cabinet est en réseau avec un antivirus « réseau » sur le serveur si l'on utilise un ordinateur portable, par définition nomade ;

[2] Voir en Annexe le BA-BA de la sécurité informatique disponible aussi sur le site de l'ordre

Attention : il faut mettre à jour régulièrement la base de données virale du logiciel et également effectuer des analyses complètes régulièrement, le mieux étant de laisser le logiciel effectuer automatiquement de manière régulière les mises à jour et analyses ;

- **Effacer les données du disque dur de l'ordinateur en cas de cession ou de mise au rebut de celui-ci** : attention, ne pas simplement « effacer » mais bien penser à vider la corbeille ; le mieux étant le formatage du disque (de la partition contenant les données, cf. infra).

1.3. Comment organiser son ordinateur pour protéger ses données ?

Il faut toujours mettre en place une séparation entre l'endroit où sont installés le système d'exploitation et les programmes (disque C :), et l'endroit où vont être sauvegardées les données (toute autre lettre que C :) : Cela permet, en cas de problème avec le système d'exploitation (Windows par exemple) qui peut engendrer un dysfonctionnement de l'ordinateur ou même une impossibilité de redémarrer, de laisser ses données « à l'abri ».

Concrètement cela impose :

- Si l'ordinateur possède plusieurs disques durs, en réserver un pour la seule sauvegarde des données et fichiers de toutes natures (textes, images, tableaux, scans etc…..) ;

- Si l'ordinateur ne possède qu'un seul disque dur (ce qui est le cas sur la plupart des portables), **effectuer dès la première utilisation** avant toute installation de programmes et sauvegarde de données une **partition du disque dur**, généralement en C : (système d'exploitation) et D : (données) : les ordinateurs sont rarement configurés de la sorte à l'achat.

  Attention, il faut ensuite configurer ses logiciels habituels de manières à ce qu'ils effectuent les sauvegardes par défaut sur D : (sinon, sous Windows par exemple, les données sont sauvegardées par défaut sur C : dans « mes documents »).

- Le complément logique et utile de cette configuration est de **sauvegarder ce que l'on appelle une « image disque » de la partition C**, que l'on peut stocker, soit sur D (s'il y a suffisamment de place), soit sur un disque dur externe (c'est mieux car plus sécurisant).
  L'avantage consiste, en cas de problème grave avec le système d'exploitation et/ou les programmes, de permettre, en très peu de temps, de « réinstaller l'ordinateur » à l'identique de la situation dans laquelle il était lors de la sauvegarde de l'image et donc, de ne pas avoir à tout réinstaller comme à l'origine (ses pilotes d'imprimantes, ses codes réseau, email, sa clé Rpva etc….).

  Attention, avant de réinstaller une image « ancienne », bien penser à sauvegarder séparément le fichier de données de ses emails (sous Outlook par exemple, le fichier outlook.pst) sous peine de perdre les emails envoyés et reçus depuis la sauvegarde de l'image disque !

1.4. Faut-il organiser une redondance des données via une sauvegarde externe ?

Il est indispensable d'organiser la redondance de ses données (toute autre lettre que C :).

Au moment où certains de nos dossiers n'existent plus que sous forme numérique, cela permet, en cas de problème avec le système d'exploitation (Windows par exemple) qui peut engendrer un dysfonctionnement de l'ordinateur ou même une impossibilité de redémarrer de laisser ses données « à l'abri ».

Concrètement cela impose :

- **D'effectuer régulièrement des sauvegardes de ses données sur un support distinct de celui utilisé tous les jours** (ordinateur) et/ou, le cas échéant, sur le serveur réseau du cabinet et/ou sur un serveur externe « cloud » (avec les problématiques nouvelles de confidentialité et de secret professionnel, cf. 2… dans l'attente de la création d'un cloud dédié aux avocats…) ;

- De considérer que tout support amovible (disque dur externe, clé USB) peut (et va certainement) un jour ou l'autre « planter » et devenir inutilisable. Il ne faut donc pas une redondance « partielle » mais totale des données ;

→ Le disque dur externe est beaucoup plus fiable qu'une simple clé USB qui ne peut, en aucun cas, servir de support de sauvegarde. Elle doit être réservée aux transferts temporaires de fichiers et données. Le disque dur externe de sauvegarde ne doit pas être transporté ou manipulé trop souvent mais être conservé dans endroit sécurisé, si possible, distinct du cabinet. Une solution toute simple consiste à disposer de deux disques durs externes étiquetés « semaine 1 » et « semaine 2 » : l'un sera branché au cabinet et sera synchronisé avec le serveur, enregistrant chaque jour toutes les données nouvelles, l'autre stocké à votre domicile. Chaque fin de semaine, on permutera les deux disques durs externes : en cas de vol, destruction (incendie) ou autre rendant inutilisable l'informatique de votre cabinet, vous n'aurez perdu qu'une semaine de données : un moindre mal qui vous évitera d'effectuer une déclaration de sinistre professionnel !

- En réseau, sauvegarder les données du serveur de manière régulière et automatique et utiliser un UPS (*Uninterruptible Power Supply*);

- Utiliser pour le branchement de tous les ordinateurs des multiprises anti-foudre avec interrupteur.

1.5. Comment protéger l'accès à distance aux ordinateurs et données du cabinet ?

- En usage « nomade » (avec un portable), l'antivirus/sécurité Internet est impérativement installé avec le firewall configuré (cf. supra);

- En réseau (filaire ou wifi), prévenir l'accès à ses fichiers en **ne partageant pas son disque et/ou ses partitions** ;

- En réseau :

  → Sécuriser l'accès physique à sa « box » Internet les codes d'accès usine figurent dessus ;

  → Configurer correctement sa « box » (que cela soit celle du cabinet ou chez soi, car rien ne sert d'appliquer des règles rigoureuses au cabinet si, lorsque l'on rapporte son ordinateur portable chez soi, son réseau personnel est vulnérable) :

    - En instaurant 2 mots de passe distincts : un **mot de passe administrateur** pour accéder à la page html de configuration de la box et **un mot de passe «réseau »** pour l'accès wifi éventuel (cf. infra) ; attention, ne pas conserver les mots de passe par défaut qui sont toujours les mêmes (Admin, User, 1234, 0000 etc….) ;

    - En activant (et en configurant) le **firewall** de la box ;

    - En activant si possible le **cryptage SSL** ;

    - En privilégiant l'accès filaire uniquement si c'est possible (prises Ethernet murales) et, dans l'affirmative, en désactivant le wifi de la box ;

  Attention : si l'accès Internet est partagé dans le cabinet, (Par exemple : plusieurs cabinets indépendants dans les mêmes locaux), il faut penser, le cas échéant, à bien séparer les réseaux des différents cabinets : c'est un sujet d'administration réseau qui suppose de configurer un routeur distinct de la box avec l'instauration de VPN et de droits utilisateurs spécifiques ; si ce n'est pas le cas, il est impératif que chaque cabinet ait sa propre box.

  Par ailleurs, il faut sécuriser les accès Ethernet filaires (prises dans les salles de réunion par exemple) qui pourraient permettre l'accès au réseau : soit en fermant les salles, soit en n'activant physiquement les prises des salles de réunion qu'en cas de besoin (dans le bandeau répartiteur derrière la box), soit en instaurant des règles logiques d'accès spécifiques (essentiellement via des routeurs externes à la box).

  → Sécuriser l'accès physique à son serveur (qui doit lui-même être équipé d'un antivirus) ;

  → Pour ce qui concerne plus spécifiquement le WIFI :

    - Masquer le nom de réseau afin qu'il ne soit pas détectable aisément (SSID) par des utilisateurs mal intentionnés (« sniffers ») ;

    - Toujours utiliser un code d'accès (relativement complexe, mêlant caractères et chiffres et en dehors des mots usuels du dictionnaire qui peuvent être trouvés par des robots), crypté de préférence en **WPA ou WPA2** (les clés WEP sont relativement facilement « cassables ») et la modifier régulièrement ; si possible, ne pas le communiquer même aux utilisateurs ;

- Configurer sa box en limitant les accès WIFI, le plus sécurisant étant le « filtrage de l'adresse MAC » (code unique identifiant chaque matériel).

2. Les fonctions externalisées

Tous les avocats ont recours à l'externalisation, qu'il s'agisse de l'externalisation des prestations juridiques qui leur ont été confiées ou de prestations purement administratives.

Cette externalisation s'effectue le plus souvent par email.

Tous les avocats sont concernés, quelle que soit la taille du cabinet, qu'ils aient une activité contentieuse ou non.

Exemples de prestations usuelles non-juridiques souvent externalisées :

Selon la taille, l'organisation et l'activité du cabinet, les prestations suivantes peuvent, et en pratique sont souvent externalisées :

- accueil ;
- standard téléphonique ;
- secrétariat ;
- reprographie ;
- entretien/ménage ;
- services informatiques ;
- comptabilité ;
- facturation ;
- paie ;
- archivage (physique ou électronique).

Exemples de prestations juridiques souvent externalisées :

Par choix ou par nécessité, les avocats sont amenés quotidiennement à externaliser les prestations suivantes :

- collaborateurs et *paralegals* ;
- postulants et correspondants, en province ou à l'étranger ;
- recours à des huissiers, notaires ou conseils en propriété industrielle ;
- professeurs de droit ;

- experts techniques et consultants divers ;
- traducteurs ;
- sténotypistes ;
- sous-traitants en matière de traitement de documents (data-room, revues d'emails, etc.).

2.1 Quels sont les risques liés à l'externalisation ?

Ils sont de deux ordres. L'externalisation des prestations juridiques et non-juridiques peut conduire l'avocat à manquer à une obligation déontologique ou professionnelle.

2.1.1 Risques déontologiques

Confidentialité/secret professionnel

L'on rappellera les dispositions très claires à cet égard de l'article 2.3 du RIN : "*L'avocat doit faire respecter le secret par les membres du personnel de son cabinet et par toute personne qui coopère avec lui dans son activité professionnelle. Il répond des violations du secret qui seraient ainsi commises …*"

Indépendance du prestataire/absence de conflit d'intérêts

L'attente légitime des clients est qu'un avocat ne soit pas en situation de conflit d'intérêts. Cette obligation s'applique à l'avocat comme à l'ensemble des membres de la structure dans laquelle il exerce, collaborateurs compris.

Il appartient à l'avocat de s'assurer auprès de tous les prestataires auxquels il s'adresse dans le cadre de l'exercice de sa mission que ceux-ci ne sont pas dans une situation de conflit d'intérêts à l'égard du client.

Obligations financières/ducroire

Dans un arrêt récent, la Cour de cassation, visant le Code de Déontologie Européen a estimé, en l'absence de disposition contractuelle particulière, que l'avocat était tenu du règlement des honoraires du correspondant étranger qu'il avait mis en rapport avec son client pour effectuer une partie d'une mission plus globale.

2.1.2 Responsabilité civile professionnelle

Sauf disposition contractuelle particulière, l'avocat est tenu à l'égard de son client à raison de la faute des prestataires auxquels il a recours.

Cette responsabilité découle, outre des règles du droit civil, des principes essentiels de compétence, de diligence et de prudence auxquels l'avocat est tenu par son serment.

2.2 Quelles questions faut-il se poser avant de s'adresser à un prestataire ?

Les questions de base que chaque avocat devrait se poser avant de recourir à un prestataire sont les suivantes :

- Le prestataire est-il fiable et compétent ?
- Va-t-il exécuter le travail lui-même ?
- Est-il soumis par son statut ou dans son pays à d'éventuelles obligations de transmission de l'information que je vais lui donner ("*disclosure*") ?
- Ses systèmes informatiques sont-ils fiables ? Sont-ils logés dans un pays "à risques" ?
- A-t-il "les reins solides" ?
- Est-il bien assuré ?
- Que va-t-il se passer à l'issue de la mission (qui paie, que devient l'information confidentielle transmise) ?

2.3 Quelles recommandations en matière d'externalisation ?

2.3.1 Information et accord du client

- Informer toujours le client au préalable de l'intervention d'un tiers dans la mission qu'il vous a confiée. C'est le seul moyen d'éviter une déconvenue.
- Essayer si possible de recueillir son accord.
- L'associer au choix du prestataire pour les prestations les plus importantes (correspondants à l'étranger, experts techniques, professeurs de droit).

2.3.2 Renseignez-vous sur votre prestataire

- Prenez soin de vous assurer par écrit de l'indépendance du prestataire au regard du client et plus généralement du dossier.
- Renseignez-vous sur :
  - le prestataire et son environnement ;
  - le risque d'une sous-traitance éventuelle de sa part ;
  - le cadre juridique local pour les prestataires basés à l'étranger (dans certains pays, les avocats peuvent être tenus de transmettre sur réquisition des informations aux autorités locales : il convient donc de s'assurer au préalable de l'existence ou non de tels risques).

2.3.3 Assurez-vous du maintien de la confidentialité

- Si votre prestataire n'est pas lui-même soumis à un secret professionnel strict, faites-lui signer un engagement de confidentialité.

- S'il existe un risque que votre prestataire puisse être tenu à une obligation de divulgation au regard de la réglementation qui lui est applicable, en informer le client et, si possible, obtenir son accord.

2.3.4 Risque que votre prestataire sous-traite la prestation ?

- Assurez-vous que le prestataire effectue lui-même la prestation.

- Interdisez la sous-traitance.

- Si celle-ci est inévitable, recueillez l'accord préalable du client. Exigez l'approbation préalable du sous-traitant par vous-même ou votre client et exigez du prestataire qu'il impose à son sous-traitant l'ensemble des conditions auxquelles il s'est lui-même engagé (confidentialité, conflit d'intérêts, etc.).

2.3.5 Qualité et responsabilité

- Assurez-vous que le prestataire et ses sous-traitants éventuels ont le niveau de compétence et la formation adéquate pour effectuer la mission confiée.

- Exigez du prestataire une assurance responsabilité civile professionnelle adéquate

2.3.6 Fin de la mission

- Assurez-vous de la protection de la propriété intellectuelle des documents confiés et des travaux accomplis.

- Assurez-vous de la restitution effective des documents ou, le cas échéant, de leur destruction.

2.4 Quels sont les risques spécifiques au *Cloud computing* ?

Le *Cloud computing* (ou informatique "en nuage") est une externalisation des serveurs informatiques hébergeant les données recueillies ou créées par l'avocat. Ces serveurs sont gérés par un ou plusieurs prestataires externes appelés hébergeurs qui peuvent eux-mêmes louer des espaces de stockage auprès d'un ou plusieurs fournisseurs.

Si le *Cloud computing* offre de nombreux avantages (réduction des coûts, simplification des systèmes informatiques et accès aux postes de travail au moyen d'une simple connexion internet), il n'est cependant pas sans risque, le plus immédiat étant l'indisponibilité temporaire des serveurs et l'un des plus graves étant le risque de divulgation d'informations confidentielles, leur perte ou leur vol.

Le consommateur de *cloud computing* n'a, *a priori*, que peu de contrôle sur la localisation ou la circulation des données stockées. International par nature, le *cloud computing* soulève au premier chef des problématiques relevant du droit des technologies de l'information qui sont encore loin d'être résolues :

- En France par exemple, les données personnelles peuvent être hébergées dans l'Espace Economique Européen ou dans certains pays considérés par l'Union Européenne comme offrant un niveau de protection équivalent à celui de l'Espace Economique Européen ("*safe harbour*") : c'est le cas des Etats-Unis si certaines conditions sont satisfaites pour l'hébergeur.

- Pour héberger des données dans d'autres pays, une autorisation de la CNIL est nécessaire.

- En Allemagne, les règles de protection sont plus strictes et il est interdit d'héberger des données en dehors des frontières nationales.

2.4.1 Quels sont les risques liés au *cloud computing* ?

Les risques sont multiples :

- risque d'ingérence d'autorités étrangères (*Patriot Act* aux Etats-Unis, par exemple) ;

- risque de divulgation d'informations confidentielles ;

- risque de saisie ;

- risque de perte ou de vol.

2.4.2 Quelles recommandations faut-il suivre en matière de *cloud computing* ?

Observant que le secret professionnel est un trait commun à tous les avocats de l'Union Européenne, le CCBE (www.ccbe.eu) a émis des recommandations visant à faciliter l'informatique en nuage tout en garantissant pour les avocats un niveau de protection maximale.

Ces recommandations sont les suivantes :

- Les avocats doivent en premier lieu s'interroger sur la question de savoir s'ils sont autorisés à conserver des données en dehors de leur cabinet.

- Ils doivent ensuite procéder à un examen préliminaire de leurs besoins : recours à des "logiciels en tant que service" (SaaS) ou à "l'infrastructure en tant que service" (IaaS).

- Ils doivent ensuite procéder à une pré-évaluation du caractère sensible des données devant être mises en nuage.

- Les avocats devront ensuite procéder à l'évaluation des normes de sécurité (ISO 27001 et 9001) du fournisseur.

- Lors de l'évaluation des services informatiques en nuage, il est prudent pour les avocats concernés de faire une comparaison entre l'infrastructure informatique du cabinet et celle du prestataire.

- Il convient également de procéder à l'évaluation de la "récupérabilité" des données en cas de défaillance du prestataire ou en cas de litige.

- Enfin, il est important de prendre un certain nombre de précautions contractuelles concernant notamment : la portée du service, la disponibilité du système, les délais de correction des erreurs, les pénalités d'inexécution ou de retard, l'évolution des besoins en matière de services, l'obligation d'adaptation à l'évolution de la réglementation, l'exclusion de l'engagement de sous-traitance sans consentement préalable, les licences, la propriété des données conservées et le droit d'accès exclusif, les accords de protection des données, les mesures de sécurité et la responsabilité, les obligations de non-divulgation, le suivi et l'élaboration de rapports, la documentation technique, le droit de contrôle et d'audit, la sauvegarde et les méthodes de récupération des données, le dépôt des logiciels à des tiers en cas d'insolvabilité ou d'incapacité commerciale de la part du fournisseur, la localisation des serveurs, les assurances, les conditions de résiliation du contrat.

- L'avocat doit en outre examiner s'il est nécessaire d'avoir une solution de rechange ou un moyen de se connecter à internet en cas de défaillance de la connexion principale.

- Enfin, afin d'assurer la transparence des services juridiques, un avocat pourrait envisager d'informer ses futurs clients que son cabinet a recours à des services d'information en nuage (mention dans la lettre de mission ou conditions générales de prestation de services).

Le CCBE reste lucide et anticipe que, dans la pratique, il ne sera pas toujours possible, pour les avocats exerçant individuellement, de satisfaire toutes ces considérations.

C'est pourquoi le Barreau de Paris, en liaison avec d'autres grands barreaux étrangers, souhaite réaliser une étude de faisabilité pour déterminer les mécanismes permettant aux avocats de respecter ces recommandations. L'idéal à terme étant en effet qu'à l'instar du RPVA, les barreaux puissent proposer aux avocats des solutions clé en main sécurisées.

3. LE SITE WEB ET LE BLOG DE L'AVOCAT

3.1. Quelles sont les règles concernant la désignation du site et le choix du nom de domaine (NDD) ?

Le nom de domaine permet d'identifier le site.

Il « ***doit comporter le nom de l'avocat ou la dénomination exacte du cabinet, qui peut être suivi ou précédé du mot « avocat ». (Article 10.6 du RIN, issu de la Décision à caractère normatif adoptée le 8 mai 2010 et publié au Journal Officiel du 11 juin 2010).***

Ce même article prévoit que le site internet de l'avocat doit être soumis au « Conseil de l'Ordre », et interdit l'usage des termes génériques, même suivis ou précédés du terme « avocat(s) ».

La Commission Publicité Démarchage et Communication est régulièrement confrontée à la problématique de « l'ancienneté » du NDD choisi par certains confrères (notamment avant la nouvelle rédaction de l'article 10.6 du RIN sus-énoncé).

Mais en l'espèce, pas de « droits acquis »… et la Commission ne peut entériner de tels noms.

Elle invite le ou les confrères concernés, à en changer.

Les sites au nom de domaines génériques font l'objet de demande de fermeture par l'Ordre.

Le terme « avocat » contenu dans le nom de domaine doit être au singulier si l'avocat exerce seul et au pluriel s'il s'agit d'un cabinet constitué de plusieurs avocats.

En effet, le site web de l'avocat est la « vitrine » de son cabinet et doit par conséquent refléter la réalité de son exercice.

Il sera ici rappelé que l'avocat a un ***devoir de probité*** et que par conséquent il ne saurait « tromper » l'internaute, en feignant d'avoir une structure différente, en l'espèce plus importante qu'elle ne l'est en réalité.

3.2. Quelles sont les règles concernant le contenu du site Web d'un avocat ?

3.2.1.- Le « corps » du site

Avant toute chose, le site doit bien identifier le ou les avocats du cabinet.

Il est par conséquent souhaitable que les noms (du cabinet et/ou des avocats) prénoms adresse et coordonnées postales et téléphoniques figurent en page d'accueil, de même que le numéro de toque. Il s'agit de permettre à l'internaute une bonne identification du cabinet.

Il n'y a pas de liste exhaustive de ce qui est autorisé, le contenu du site est « libre », sous réserves de ne pas contenir de mentions interdites (article 10.4 du RIN et P10 du RIBP).

Toutefois, il doit être « véridique » et bien entendu respecter les principes essentiels.

Ainsi, à titre d'exemple, l'avocat, qui doit toujours faire preuve de ***conscience et de probité***, ne saurait faire valoir une « spécialisation » alors qu'il n'est pas titulaire du certificat y relatif, quand bien même son activité serait exclusive dans une matière, et ce, même de longue date.

Il en va de même pour le cabinet qui ne peut en aucun cas être « spécialisé », car seule la personne physique titulaire d'un certificat l'est, sauf à ce que tous les membres du cabinet soient titulaires dudit même certificat.

L'avocat ne peut se prévaloir d'être le conseil de tel ou tel prestigieux client, même si cela lui procure une publicité supplémentaire.

En effet, cette interdiction résulte de l'article 2.2 du RIN, relative au ***secret professionnel*** de l'avocat. Seule exception, en matière d'appels d'offres.

Telle est la règle rappelée récemment par Monsieur le Bâtonnier POIRIER, Président de la Commission Règles et Usages du C.N.B, le 5 septembre 2013, interrogé sur la question.

S'agissant de la publication des « tarifs » ou des honoraires pratiqués, dans le marché très concurrentiel d'aujourd'hui, certains confrères n'hésitent pas à avoir de véritables « prix d'appels » telles des promotions commerciales. Or, précisément, ces pratiques remettent en cause l'essence même de la profession, s'agissant du principe de la fixation de l'honoraire.

Certains confrères, soucieux d'être « plus attractifs », proposent, sur leur site, la possibilité de régler les honoraires en plusieurs fois.

Or, si la pratique est amplement tolérée, voire nécessaire pour certains clients, elle n'en demeure pas moins, contraire aux articles L131-31 et L131-32 du code monétaire et financier.

Il en est de même pour la « première consultation gratuite » affichée par de nombreux sites.

Si l'avocat est libre de fixer ses honoraires comme il l'entend, voire y renoncer purement et simplement, pour autant, publier une telle « proposition » est susceptible de constituer un acte de concurrence déloyale vis-à-vis des confrères.

Enfin, le contenu du site de l'avocat ne doit pas contenir de mentions laudatives (article 10.2 du RIN).

3.2.2. Les liens hypertextes

Beaucoup de sites comportent des liens hypertextes.

Si certains ne posent pas de difficultés (notamment les liens vers des sites dits « institutionnels » : Infogreffe, Legifrance, Ordre des Avocats, CNB…), d'autres oui.

Il est à noter que souvent les confrères prévoient, dans l'onglet « mentions légales » notamment, une exclusion de responsabilité quant au contenu des sites vers lesquels ils ont créé un lien hypertexte. Prudence, sagesse ou méconnaissance ?

Au terme de l'article 10.6 alinéa 6 de notre Règlement :

« Le site de l'avocat ne peut comporter de liens hypertextes permettant d'accéder directement ou indirectement à des sites ou à des pages de sites dont le contenu serait contraire aux Principes Essentiels de la profession d'avocat. »

Il appartient à l'avocat d'y veiller et, plus généralement, de faire une déclaration préalable de tout lien hypertexte qu'il envisagerait de créer.

Dès lors, mieux veut se limiter à des liens hypertextes vers des sites dits « institutionnels » ou renoncer à de tels liens.

Les liens hypertextes vers des pages personnelles de réseaux sociaux peuvent également poser d'importantes difficultés, et ce, notamment au regard du ***devoir de dignité de l'avocat***, qui fera preuve de la plus grande prudence quant à l'éventuel « mélange des genres » entre sa vie professionnelle et sa vie personnelle.

3.3. A quoi servent les «Mentions légales » ? Sont-elles obligatoires ?

L'onglet comportant les « mentions légales » est obligatoire. Ces mentions permettent d'identifier plus précisément le cabinet et le responsable de publication du site.

En application de l'article 6.III de la loi 2004-575 du 21 juin 2004, l'onglet « mentions légales » doit préciser :

- La dénomination et la raison sociale du cabinet ;
- L'adresse du siège social ;
- Les coordonnées postales, téléphoniques et électroniques (adresse mail) ;
- Nom et coordonnées du directeur de publication du site (webmaster) ;
- Nom, raison sociale, adresse et coordonnées de l'hébergeur du site.

3.4. Comment se déroule la procédure de validation d'un site Web d'avocat par l'ordre ?

Théoriquement, avant toute mise en ligne, l'avocat doit soumettre à l'Ordre, pour validation, son site internet et à tout le moins sa maquette (article 10.6 du RIN). En pratique, tel n'est pas toujours le cas.

L'avocat doit donc soumettre son site à l'appréciation de l'Ordre.

Concrètement l'avocat saisit l'Ordre en communiquant son nom de domaine et sa maquette, en adressant un mail au service de déontologie (delegationgenerale@avocatparis.org) comportant un lien vers le site que l'avocat se propose de mettre en ligne.

Le dossier est ouvert et transmis à la Commission Publicité Démarchage et Communication.

En premier lieu, c'est le nom de domaine qui est validé ou invalidé, notamment en cas de pluriel au terme avocat si, après vérification, l'intéressé exerce seul.

Puis, c'est le contenu qui est analysé : présence de l'onglet « mentions légales » et conformité des mentions (notamment absence d'exclusion de responsabilité concernant les liens hypertextes), le contenu du site est lu intégralement, de sorte à vérifier l'absence de mentions interdites.

Quand le site ne pose aucune difficulté, il est immédiatement validé et le cabinet reçoit un courrier de validation, l'invitant à en transmettre copie au SEP (Service de l'Exercice Professionnel), de sorte à ce que le nom de domaine de l'avocat (ou du cabinet) soit enregistré, comme élément supplémentaire d'identification.

Le site peut ensuite être mis en ligne et faire l'objet de la mention suivante : *« Site validé par l'Ordre des Avocats de Paris »*.

Quand le site comporte des mentions interdites, il donne lieu à un échange de correspondances plus ou moins foisonnant et plus ou moins long, avec l'intéressé.

En cas de refus ou d'absence de modifications pour rendre le site conforme, il reste possible d'envisager une éventuelle transmission au service disciplinaire pour que l'avocat concerné défère aux demandes de modifications.

Bien entendu, la vérification et la validation de site n'est réalisée qu'à un instant « t »…alors même que le site peut être modifié à tout moment…

3.5. Un avocat doit-il soumettre son blog au contrôle de l'ordre ?

A l'heure actuelle, les blogs font simplement l'objet d'un ***enregistrement.***

Il est rappelé aux confrères qu'ils doivent faire preuve de prudence dans leurs propos, et toujours veiller à respecter les principes essentiels (article 10.6 du RIN dernier alinéa).

Or, par essence, le blog est évolutif et modifié plus ou moins régulièrement, selon la constance et l'intérêt que lui porte son titulaire.

Dès lors, même à un instant « t », l'analyse d'un blog présente un caractère tout à fait relatif.

Dans ces conditions, il est peu aisé de « valider » un blog, sauf à en faire une page figée, annihilant ainsi son sens même.

La même problématique se pose pour les réseaux sociaux…

3.6. La publicité est-elle autorisée pour les avocats ?

Oui, la publicité est permise à l'avocat sous certaines conditions spécifiques (articles 10 et suivants du R.I.N), mais doit, avant publication ou mise en ligne, être soumise à la validation de l'Ordre (article 10.1 du R.I.N).

3.7. Un site internet, à quelle fin ?

Assurer l'information du public, dans le respect des principes essentiels de la profession.

3.8. L'avocat peut-il choisir le nom de domaine de son site, et dans l'affirmative, selon quels critères ?

Le choix est limité au nom de l'avocat ou la dénomination exacte du cabinet, qui peut être suivi ou précédé du mot « avocat(s) ».

3.9. Peut-on employer, dans le nom de domaine, le terme « avocat » au pluriel ?

Oui, ***si et seulement si*** le site concerne un cabinet constitué de plusieurs avocats.

A défaut, le terme « avocat » doit être au singulier.

Le site de l'avocat doit refléter, avec exactitude, l'activité et le mode d'exercice de l'avocat, faute de quoi, il trompe le public. Le site web de l'avocat est la « vitrine » de son cabinet et doit par conséquent refléter la réalité de son exercice.

Il sera ici rappelé que l'avocat a un ***devoir de probité*** et que par conséquent il ne saurait « tromper » l'internaute, en feignant d'avoir une structure différente, en l'espèce plus importante qu'elle ne l'est en réalité.

3.10. Peut-on ajouter, dans le nom de domaine, des termes génériques, pour préciser un domaine de compétence ou une spécialité ?

Non, car « l'*utilisation des noms de domaine évoquant de façon générique le titre d'avocat ou un titre pouvant prêter à confusion, un domaine du droit ou une activité relevant de celles de l'avocat est interdite* » (article 10.6 du RIN).

3.11. Peut-on se prévaloir de l'antériorité d'un nom de domaine non conforme, pour le garder ?

Non, il n'y a pas de droit acquis en la matière, l'avocat doit respecter toutes les dispositions du droit positif.

3.12. Peut-on faire de la publicité informative en étant intégré à un site de référencement ?

Oui, la publicité informative est autorisée tant sur les sites de référencement (depuis un avis du CNB en date du 11 janvier 2008, publié au JO du 11 juin 2008), avec possibilité de préciser les « activités dominantes » ou activités pratiquées. La même publicité est autorisée sur les annuaires professionnels.

Il faut également signaler qu'il existe sur internet de prétendus annuaires professionnels, qui n'en sont pas.

L'Ordre est régulièrement saisi par des confrères inscrits à leur insu sur ces sites, avec des coordonnées incomplètes ou erronées, mais surtout avec des numéros de téléphone qui renvoient à des plateformes téléphoniques aux numéros surtaxés.

3.13. Dans quelles conditions peut-on mettre en ligne son site internet ?

« L'avocat qui ouvre ou modifie un site internet doit en informer le Conseil de l'Ordre sans délai et lui communiquer les noms de domaine qui permettent d'y accéder. » (Article 10.6 du RIN)

Si le texte dit « sans délai », il est préférable et plus prudent de soumettre à l'Ordre, son site ou sa maquette de site, avant toute mise en ligne, tant pour s'assurer de sa conformité, en amont, que pour éviter des modifications, après la mise en ligne, et le coût y relatif.

Concrètement l'avocat saisit l'Ordre en communiquant son nom de domaine et sa maquette, en adressant un mail au service de déontologie (delegationgenerale@avocatparis.org) comportant un lien vers le site que l'avocat se propose de mettre en ligne.

3.14. Y a-t-il des mentions obligatoires à intégrer en page d'accueil ?

Oui, le cabinet doit être immédiatement et clairement identifié.

Les mentions obligatoires sont identiques à celles qui sont obligatoires pour le papier à lettre (adresse du cabinet, nom et prénom de l'avocat, barreau d'appartenance, numéro de téléphone et de télécopie, dénomination du cabinet s'il y a lieu, type de structure d'exercice).

3.15. Quelles informations peut-on diffuser ou publier ?

Outre l'identification complète du Cabinet, le site peut contenir de nombreuses informations, d'ordre général ou plus ciblées, par matière, par type de contentieux.

Le site peut également contenir une actualité jurisprudentielle.

La publicité à travers le site internet « *inclut la diffusion d'informations sur la nature des prestations de services proposées, dès lors qu'elle est exclusive de toute forme de démarchage.*

Cette publicité doit être véridique, respectueuse du secret professionnel et mise en œuvre avec dignité et délicatesse ».

3.16. Peut-on utiliser le terme de spécialiste en une ou plusieurs matières ?

Oui, ***si et seulement si*** on est – ***effectivement*** – titulaire du certificat de spécialisation y afférent.

A défaut, cette mention est interdite (***devoir de conscience et probité***).

3.17. Le cabinet peut-il être qualifié de « spécialiste » ?

Non. Seule une personne physique titulaire du certificat de spécialisation, peut être qualifiée de « spécialiste ».

Seul tempérament : si ***tous*** ses membres du cabinet sont titulaires d'un même certificat de spécialisation.

3.18. Comment l'Ordre vérifie-t-il la conformité du site ?

Le dossier est ouvert et transmis à la Commission Publicité Démarchage et Communication.

C'est d'abord le nom de domaine qui est validé ou invalidé.

Puis, c'est le contenu qui est analysé : présence de l'onglet « mentions légales » et conformité des mentions (notamment absence d'exclusion de responsabilité concernant les liens hypertextes), le contenu du site est lu intégralement, de sorte à vérifier l'absence de mentions interdites.

Quand le site ne pose aucune difficulté, il est immédiatement validé et le cabinet reçoit un courrier de validation, l'invitant à en transmettre copie au SEP (Service de l'Exercice Professionnel), de sorte à ce que le nom de domaine de l'avocat (ou du cabinet) soit enregistré, comme élément supplémentaire d'identification.

Le site peut ensuite être mis en ligne et faire l'objet de la mention suivante : *« Site validé par l'Ordre des Avocats de Paris »*.

3.19. Doit-on soumettre la modification de son site internet à la validation de l'Ordre ?

Toute mise à jour modifiant de façon substantielle le contenu du site et pouvant être de nature à justifier une nouvelle validation de l'Ordre ***doit*** faire l'objet d'une nouvelle demande de validation.

3.20. Peut-on mentionner le nom de client(s), avec l'accord de celui/ceux-ci ?

Non, l'avocat ne peut se prévaloir d'être le conseil de tel ou tel client, prestigieux ou pas, même si cela lui procure une publicité supplémentaire.

En effet, cette interdiction résulte de l'article 2.2 du RIN, relative au ***secret professionnel*** de l'avocat. Seule exception, en matière d'appels d'offres, avec l'accord du client.

Telle est la règle rappelée récemment par Monsieur le Bâtonnier POIRIER, Président de la Commission Règles et Usages du C.N.B, le 5 septembre 2013, interrogé sur la question.

3.21. Quelles sont les mentions de l'onglet « mentions légales » obligatoire ?

L'onglet « mentions légales » doit préciser (Article 6.III de la loi 2004-575 du 21 juin 2004) :

- La dénomination et la raison sociale du cabinet ;
- L'adresse du siège social ;
- Les coordonnées postales, téléphoniques et électroniques (adresse mail) ;
- Nom et coordonnées du directeur de publication du site (webmaster) ;
- Nom, raison sociale, adresse et coordonnées de l'hébergeur du site.

3.22. Quelles sont les mentions prohibées ?

Comme pour toute publicité, sont prohibés :

- les renseignements inexacts ou mensongers ;
- les termes laudatifs et/ou comparatifs ;
- les mentions susceptibles de créer, dans l'esprit du public, l'apparence d'une structure ou de qualifications inexistantes ou erronées ;
- toutes références à des fonctions ou des activités sans lien avec la profession ;
- toutes mentions susceptibles de porter atteintes au secret professionnel.

Sont également prohibés les encarts ou bannières publicitaires pour quelques activités et/ou produits que ce soit.

3.23. Peut-on utiliser un logo ? Lequel ?

Il est possible d'utiliser le logo créé pour le cabinet, à condition que celui-ci ne contienne pas de signes ou de significations qui seraient contraires à nos principes essentiels.

Il est également possible d'utiliser les logos mis à disposition par le CNB.

En revanche, il n'est en aucun cas possible d'utiliser le logo de l'Ordre des Avocats de Paris, qui est sa ***propriété exclusive.***

3.24. Quelles précisions l'avocat peut-il mentionner sur son site concernant les honoraires ?

La fixation du montant des honoraires est libre, l'article 11.1 du RIN prévoit : *« à défaut de convention entre l'avocat et son client, les honoraires sont fixés selon les usages, en fonction de la situation de fortune du client, de la difficulté de l'affaire, des frais exposés par l'avocat, de la notoriété et des diligences de celui-ci (…) »*.

Le mode de facturation, le tarif horaire et la possibilité d'établir une convention d'honoraire peuvent être développé sur le site de l'avocat.

3.25. Peut-on proposer un règlement des honoraires en plusieurs échéances ?

Non, en aucun cas.

Il convient de rappeler que si les avocats peuvent accepter que leurs honoraires soient réglés en plusieurs fois, ils ne sauraient en faire état sur leur site, sauf à contrevenir aux articles L. 131-31 et L. 131-32 du Code monétaire et financier.

Si la pratique est tolérée, voire nécessaire pour certains clients, elle n'en demeure ainsi pas moins contraire à ces dispositions.

3.26. Peut-on proposer une « première consultation gratuite » ?

Non, en aucun cas.

Si l'avocat est libre de fixer ses honoraires comme il l'entend, voire y renoncer purement et simplement, pour autant, publier une telle « proposition » est susceptible de constituer un acte de concurrence déloyale vis-à-vis des confrères.

3.27. L'avocat peut-il créer librement des liens hypertextes sur son site internet d'avocat ?

Librement, non.

Si certains sites ne posent pas de difficultés (notamment les liens vers des sites dits « institutionnels » : Infogreffe, Legifrance, Ordre des Avocats, CNB…), d'autres oui.

*« Le site de l'avocat ne peut comporter de liens hypertextes permettant d'accéder directement ou indirectement à des sites ou à des pages de sites **dont le contenu serait contraire** aux Principes Essentiels de la profession d'avocat. »*

Il appartient à l'avocat d'y veiller et, plus généralement, de faire une déclaration préalable de tout lien hypertexte qu'il envisagerait de créer.

En tout état de cause, l'avocat se doit de vérifier régulièrement tant le contenu de son propre site que le contenu de tout site vers lequel il disposerait d'un lien hypertexte.

Les liens hypertextes simples, sont susceptibles de porter atteinte aux droits d'auteurs ou de constituer des pratiques de concurrence déloyale (lien profond ou deep linking).

Dès lors, il reste préférable de se limiter à des liens hypertextes vers des sites dits « institutionnels » ou renoncer à de tels liens.

3.28. Quid d'un lien hypertexte vers une page de réseau social ?

Il ne peut qu'être appelé à la plus grande prudence sur la communication de l'avocat sur les réseaux sociaux et par conséquence sur le renvoi sur le site internet de l'avocat ou du cabinet par un lien hypertexte sur une page de réseau social.

Les liens hypertextes vers des pages personnelles de réseaux sociaux peuvent poser d'importantes difficultés, et ce, notamment au regard du ***devoir de dignité de l'avocat***.

Le cas échéant, il convient de faire preuve de la plus grande prudence quant à l'éventuel « mélange des genres » entre sa vie professionnelle et sa vie personnelle.

3.29. Peut-on prévoir une exclusion de responsabilité, concernant les liens hypertextes présents sur le site et renvoyant vers des sites tiers ?

Non, en aucun cas.

Il ne peut être dérogé à l'article 10.6 du RIN qui prévoit, précisément, un contrôle par l'avocat, des sites tiers vers lesquels il créé un lien hypertexte.

3.30. Est-on plus « libre de ses propos » sur un blog que sur un site ?

Non.

L'avocat doit toujours faire preuve de prudence dans ses propos et veiller à respecter les principes essentiels (article 10.6 du RIN dernier alinéa).

4. RESEAUX SOCIAUX

4.1. Quels sont les principes généraux à respecter en matière de référencement ?

La présence d'un avocat sur un réseau social s'apparente à une forme de publicité personnelle, dès lors qu'il est fait état de sa qualité d'avocat. Elle est donc soumise aux règles en la matière et notamment à l'article 10 du RIN.

Conformément à l'article 10.6 du RIN, *« L'avocat participant à un blog ou à un réseau social en ligne doit respecter les principes essentiels de la profession ainsi que l'ensemble des dispositions du présent article. ».*

Aux termes des articles 10.1 et 10.2. du RIN, la publicité est permise à l'avocat si elle procure une information au public et si sa mise en œuvre respecte les principes essentiels de la profession, sous réserve que leur présentation, leur emplacement ou leur contenu ne soit pas de nature à induire le public en erreur ou à constituer un acte de concurrence déloyale.

Article 184 Décret de 1991 : « Toute contravention aux lois et règlements, toute infraction aux règles professionnelles, tout manquement à la probité, à l'honneur ou à la délicatesse, même se rapportant à des faits extraprofessionnels, expose l'avocat qui en est l'auteur aux sanctions disciplinaires énumérées à l'article 184. »

Les principes essentiels de la profession d'avocat s'appliquant tant dans la vie personnelle que professionnelle.

Cela vise tant :

- les pages cabinet, purement professionnelles,

- les pages personnelles,

- les pages mixtes.

L'avocat est tenu d'un devoir de prudence renforcé sur les réseaux sociaux, tant en raison des informations ou écrits qu'il pourrait y publier, qu'en raison de ceux qui pourraient être publiés par des tiers sur sa propre page.

4.2. Quels sont les points à vérifier concernant le contenu du « profil » ou d'une page d'un réseau social, pour s'assurer que ce contenu soit conforme à nos règles déontologiques.

Sont prohibés sur les réseaux sociaux :

- toute publicité mensongère ou contenant des renseignements inexacts ou fallacieux

- toutes références à des fonctions ou activités sans lien avec l'exercice de la profession d'avocat ;

- toutes mentions laudatives ou comparatives

- toutes mentions susceptibles de créer l'apparence d'une qualification professionnelle non reconnue

- toutes mentions susceptibles de porter atteinte au secret professionnel

- toutes indications contraires à la loi (art. 10.2 RIN).

4.3. Quelles formalités déclaratives auprès de l'Ordre effectuer ?

La création d'un profil ou l'adhésion à un réseau social n'a pas à faire l'objet d'une déclaration auprès de l'Ordre. En cas de doute sur la licéité du contenu d'un profil ou sur la possibilité d'apparaitre sur certains réseaux sociaux en qualité d'avocat, il est toujours possible d'interroger l'Ordre par un mail adressé au service de déontologie (delegationgenerale@avocatparis.org) comportant un lien vers le profil ou la page d'accueil du réseau concerné.

4.4. Peut-on avoir comme contact un client ? Un magistrat ?

Le secret professionnel de l'avocat comporte en principe le nom des clients de l'avocat. Ainsi, dans l'hypothèse où une liste de « contact clients » existerait, il appartient à l'avocat de protéger celle-ci au même titre que le secret professionnel. Il n'est donc pas possible de faire figurer le nom de ses clients comme tel sur un réseau social.

De même, s'il n'est pas interdit de mentionner comme contact (« ami » sur FaceBook par exemple) le nom d'un magistrat ou tout autre professionnel (expert agréé, notaire, etc.), cela doit être fait de façon neutre, sans mise en avant par l'avocat des fonctions ou profession de ses contacts. En tout état de cause, la mention du nom et a fortiori de la qualité d'une personne présentée comme un contact ne peut être fait qu'avec son accord (acceptation de la « demande de mise en relation » sur Linkedin par exemple).

4.5. Peut-on se faire recommander par un client sur un réseau social ?

Le secret professionnel de l'avocat comporte en principe le nom des clients de l'avocat et son agenda. Pour autant, rien n'interdit le client, qui n'est pas tenu au secret professionnel, de dévoiler le nom de son avocat et de porter une appréciation sur ce dernier.

5. LE REFERENCEMENT

5.1. Quels sont les principes généraux à respecter en matière de référencement ?

Le référencement s'apparente à de la publicité. Il prend notamment la forme de liens hypertextes, liens sponsorisés (backlinks) ou achat de mots clés, générateur automatique de liens, balises métadonnées, code Javascirpt. Il est donc soumis aux règles en la matière et notamment à l'article 10 du RIN.

L'article 10.6 du RIN précise que le site d'un avocat : *« L'utilisation de noms de domaine évoquant de façon générique le titre d'avocat ou un titre pouvant prêter à confusion, un domaine du droit ou une activité relevant de celles de l'avocat, est interdite. »*

Jugé que : *« l'évidence d'un lien informatique entre le site de M. X... et le nom "de Y..." comme unique critère de recherche et relevé que ce rapprochement, de nature à créer une confusion entre deux avocats ayant la même activité spécialisée, était à l'origine d'un trouble manifestement illicite »* (Civ. 2 12 Juillet 2012, n°11-20.287, Bull. n°133).

5.2. Un avocat peut-il acheter des mots clés sur internet (par le moyen de liens sponsorisés) pour accroitre la visibilité de son cabinet ?

Oui mais l'avocat ne peut pas acheter ou utiliser n'importe quel mots-clés.

L'utilisation de mots clés en tant qu'elle induit un rattachement de l'avocat aux mots clés utilisés ou achetés, ne doit pas porter atteinte aux droits des marques, à la renommée d'autrui, aux droits d'auteurs. Elle ne doit pas conduire non plus à constituer un dénigrement ou un acte de concurrence déloyale.

L'utilisation de mots clés de nature à induire en erreur est prohibée. Tel est le cas si les mots clés concernés rattachent l'avocat à un département dans le ressort duquel il n'est pas inscrit ou ne possède pas de bureau secondaire (art. 10.5. du RIN), renvoi à une spécialisation dont il n'est pas titulaire (art. 10.4.3. et 10.5. RIN), …

Sont ainsi prohibés l'achat de mots clés tels que « ordre des avocats de … », « membre du conseil de l'ordre de … », « meilleur avocat en … », « avocat spécialisé en … », du nom d'un confrère renommé, ou d'un cabinet concurrent,

L'utilisation de noms de domaine évoquant de façon générique le titre d'avocat ou un titre pouvant prêter à confusion, un domaine du droit ou une activité relevant de celles de l'avocat, est interdite (10.6. RIN).

NB : si l'achat de mots-clés garantissait initialement un meilleur référencement sur le Net, la croissance exponentielle du nombre de sites, a peu à peu diminué l'intérêt d'un tel achat. En effet, loi de l'offre et de la demande oblige : de plus en plus de créateurs de sites acquièrent des mots-clés, souvent similaires dans un même secteur d'activité, sans pour autant avoir quelque garantie que ce soit d'obtenir le « meilleur » et à tout le moins un « bon » référencement. Méfiance donc !

5.3. Puis-je faire librement des liens hypertextes sur mon site internet ? Quelles sont les règles qu'il convient d'observer à ce sujet ?

L'article 10.6 du RIN précise que : *« Le site de l'avocat ne peut comporter aucun encart ou bannière publicitaire, autres que ceux de la profession, pour quelque produit ou service que ce soit.*

Il ne peut comporter de lien hypertexte permettant d'accéder directement ou indirectement à des sites ou à des pages de sites dont le contenu serait contraire aux principes essentiels de la profession d'avocat. Il appartient à l'avocat de s'en assurer en visitant régulièrement les sites et les pages auxquelles permettent d'accéder les liens hypertexte que comporte son site, et de prendre sans délai toutes dispositions pour les supprimer si ce site devait se révéler contraire aux principes essentiels de la profession.

Il appartient à l'avocat de faire une déclaration préalable au conseil de l'Ordre de tout lien hypertexte qu'il envisagerait de créer. »

Les liens hypertextes simple, sont susceptibles de porter atteinte aux droits d'auteurs ou de constituer des pratiques de concurrence déloyales (lien profond ou deep linking).

6. L'activité de l'avocat via des sites tiers et l'intermédiation

6.1. Les prestations juridiques en ligne sont-elles autorisées ? Quelles règles leurs sont applicables ?

La fourniture de prestations juridiques en ligne est autorisée mais réglementée par les dispositions de l'article 6.6 du RIN et l'article 161 du décret du 27 novembre 1991.

Elle se définit comme la fourniture d'un service personnalisé de l'avocat à un client habituel ou nouveau. L'avocat qui participe au site Internet d'un tiers, y est référencé ou visé par un lien hypertexte, doit vérifier que son contenu est conforme aux principes qui régissent la profession, et en informer l'Ordre. Il doit également s'assurer que les prestations juridiques relèvent du seul domaine de l'information juridique.

Cette obligation de vérification de l'avocat doit porter sur le contrôle permanent du contenu du site et sur son mode de fonctionnement, dont la publicité qui en est faite par l'entreprise gestionnaire. L'attention des avocats est notamment attirée sur le fait que certains de ces sites internet tiers proposent directement des prestations juridiques, agissements susceptibles de constituer des infractions pénales.

La prestation doit être effectuée dans le respect du secret professionnel et de la règle du conflit d'intérêt.

Si tel n'est pas le cas, il doit cesser son concours (art. 6.6.4.3, dernier alinéa RIN).

6.2. Puis-je répondre à des questions posées sur un site par des internautes anonymes ?

Oui, s'il s'agit de questions d'ordre général, notamment sur des forums de discussion ou qui seront accessibles à d'autres internautes. Il faudra veiller à donner des réponses générales, l'avocat devant toujours rester prudent.

Dans le cadre d'une consultation non publique l'avocat doit connaître l'identité de l'internaute car il est toujours tenu d'éviter tout conflit d'intérêt y compris en matière juridique.

Dans tous les cas, l'avocat doit, en toute circonstance, être clairement identifié permettant ainsi au public de vérifier notamment son identité et sa qualité, auprès de son ordre.

6.3. A quelles conditions l'avocat peut-il fournir une consultation en ligne ?

Pour respecter les principes d'indépendance et de secret professionnel ainsi que pour éviter des conflits d'intérêts et plus généralement pour respecter les principes essentiels de dignité, de confiance, de compétence et de prudence (art. 1.3 du RIN) l'avocat doit s'assurer de l'identité de la personne à laquelle il répond. Et, inversement l'avocat qui répond doit toujours être identifiable et son nom communiqué à l'internaute avant la fourniture de toute prestation juridique.

Afin notamment de respecter le secret professionnel et d'éviter le conflit d'intérêt, l'avocat devra donc :

- s'assurer de l'identité et des caractéristiques de la personne à laquelle il répond,
- fournir des informations adaptées à la situation de l'interrogateur,
- être toujours en mesure d'entrer personnellement et directement en relation avec l'internaute, notamment pour poser les questions complémentaires nécessaires conduisant à la fourniture d'un service adapté aux besoins de l'internaute.

D'une façon plus générale, le fait pour un avocat de proposer ses diligences en ligne par l'intermédiaire d'un site internet implique qu'il s'interroge sur la conformité d'une telle pratique eu égard à l'encadrement de la publicité et du démarchage, à son devoir de conseil et de prudence et au respect du principe de dignité et à l'absence de conflit d'intérêt.

Fréquemment se posera également la question du consentement car l'outil informatique ne permet pas d'en établir la réalité avec certitude. A titre d'exemple, la commission plénière de déontologie a considéré dans un avis rendu le 2 octobre 2012 qu'il n'était pas possible de préparer une audience en divorce sur consentement mutuel sans rencontrer préalablement le client, l'interactivité limitée des échanges par le biais de l'internet ne permettant pas le respect de nos principes essentiels. A cette occasion, la Commission plénière de déontologie a estimé que les dispositions des articles 6.6.1 et suivant du RIN régissaient exclusivement l'activité juridique et non judiciaire.

6.4. A quelles conditions un avocat peut-il percevoir des rémunérations pour ses prestations en ligne ?

Un avocat peut créer un site internet de prestations juridiques, de sorte qu'il peut librement percevoir toute rémunération des clients de ce site (article 6.6.4.1), le cas échéant par l'intermédiaire d'un établissement financier assurant la sécurité des paiements en ligne, pour autant que l'identification du client reste aussi possible à cette occasion.

L'avocat peut également intervenir sur un site tiers dit « d'intermédiation », sous certaines conditions.

Tout d'abord, il fera une déclaration à l'Ordre concernant son intervention sur ledit site tiers, en joignant à sa déclaration le contrat passé avec ledit site.

L'avocat devra à cette occasion vérifier que la convention (ou les condition général d'utilisation du site)ne porte pas atteinte à la liberté de fixation de ses honoraires en accord avec son client, **toute fixation forfaitaire des honoraires par un tiers étant contraire au principe d'indépendance de l'avocat**.

De même, le versement des honoraires à l'avocat par l'intermédiaire du site d'intermédiation est prohibé par les dispositions de l'article P.11.6.0.1, le site d'intermédiation ne pouvant être le tiers payeur au sens de ce texte.

L'avocat peut être amené à participer de façon forfaitaire aux frais de fonctionnement de ce site à l'exclusion de toute rémunération qui serait établie en fonction des honoraires qu'il percevrait des clients avec lesquels le site l'a mis en relation.

L'avocat se voyant diriger de façon régulière des clients par le biais d'un site d'intermédiation doit également veiller à conserver son indépendance économique vis-à-vis dudit site.

Il appartient au Bâtonnier de demander à l'avocat communication du contrat en cas de doute sur le respect des principes ci-dessus rappelés.

6.5. Un site tiers peut-il collecter des données ou des documents d'un client et les transmettre à l'avocat référencé sur ce site ?

Non car l'immixtion du site d'intermédiation dans la relation entre le client et l'avocat constituerait une violation du secret professionnel, un site d'intermédiation ne pouvant que mettre l'avocat en relation avec un client mais non contribuer d'une quelconque façon que ce soit à la réalisation de la prestation de l'avocat qui doit en avoir la complète maîtrise.

Une fois que la mise en relation entre l'internaute et l'avocat a été réalisée, l'avocat doit se retrouver dans la configuration « classique » et secrète de la relation avec son client, à l'exclusion de tout intervention d'un tiers.

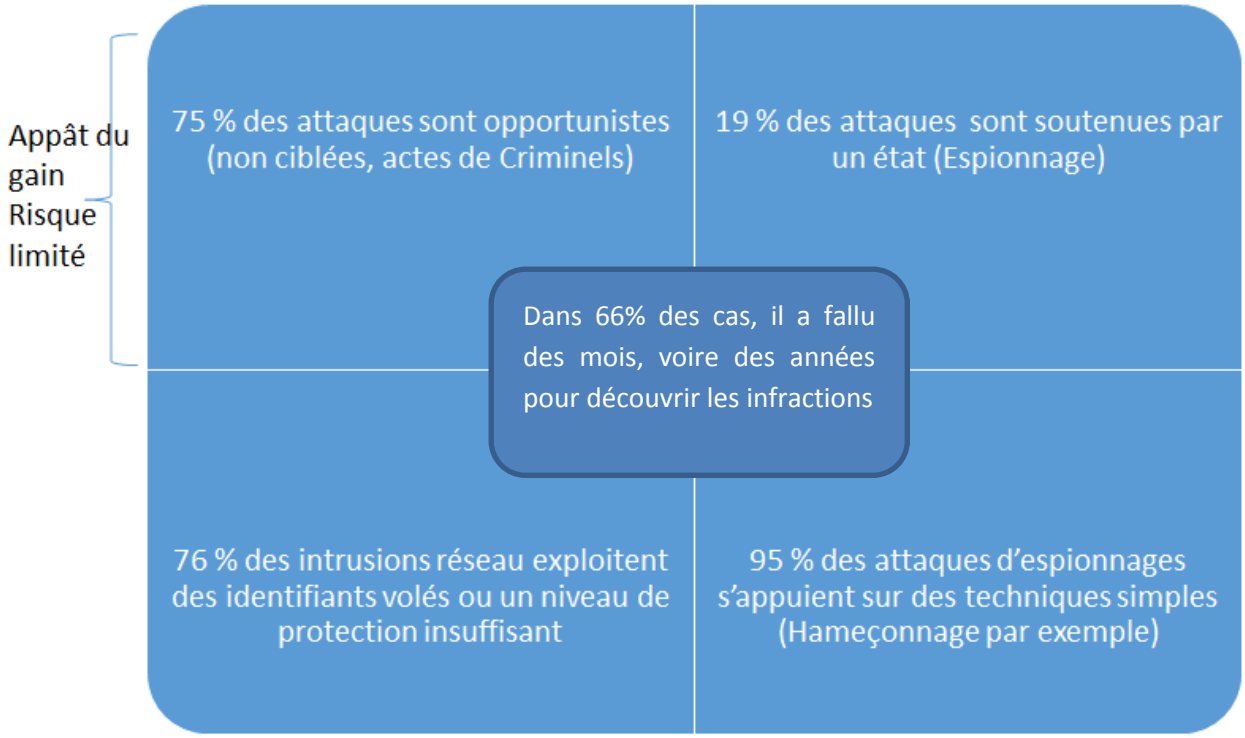
ANNEXE : LE BA-BA DE LA SECURITE INFORMATIQUE

Parce que le respect de la déontologie est aussi une affaire de sécurité, chaque avocat pourra se reporter utilement à la présente annexe qui reprend le BA-BA de la sécurité informatique disponible sur le site de l'ordre.

A. Un tour d'horizon de la sécurité informatique (SI)

I. Quelques chiffres

i. Source : Rapport VERIZON DBIR 2013 (47 000 incidents de sécurités analysés, 19 pays)



II. Situation des entreprises en France et dans le monde

I. Le centre d'analyse stratégique (remplacé par le Commissariat général à la stratégie et à la prospective depuis le 17 avril), dans sa note du 19 mars 2013, dit :

- Les organisations sont insuffisamment protégées pour faire face à des attaques informatiques de plus en plus élaborées. Élever le niveau de cybersécurité est une urgence pour préserver la compétitivité économique et la souveraineté nationale.

• Confrontés à cette menace, les entreprises, les administrations et *a fortiori* les particuliers sont soit désarmés, soit peu conscients des risques encourus et de leurs conséquences économiques et financières. Des attaques informatiques peuvent piller le patrimoine informationnel des entreprises et toucher des infrastructures stratégiques. Le Livre blanc sur la défense et la sécurité nationale paru en 2008 avait ainsi consacré la sécurité des systèmes d'information comme l'une des quatre priorités stratégiques pour la France : c'est un enjeu de compétitivité et de souveraineté nationale.

• Pour élever le niveau de sécurité, tout en tirant profit des avantages d'un Internet ouvert et décentralisé, les organisations doivent adopter une démarche rationnelle d'analyse de risques afin de mettre en œuvre une réponse adaptée sur le plan technique et organisationnel.

II. La société symantec, dans son rapport du 16 avril 2013 :

• croissance du nombre de cyberattaques ciblées enregistrées en 2012 : + 42 %

• Les PME ont vu le nombre d'attaques les visant multipliées par trois entre 2011 et 2012

III. L'avocat est-il concerné ?

• La sécurité et la confidentialité des données est un enjeu pour toutes les entreprises. Les avocats sont soumis au secret professionnel.

• Des risques et des responsabilités, quel que soit le mode d'exercice professionnel.

• L'enjeu est également celui de la confiance avec le client.

• Matérialisation du risque : perte de données, fuite et vol d'informations.

B. Comment se protéger, quelques règles de base

I. Classification des données

Niveau 0 : Information « publique »

Les informations publiques peuvent être ouvertes au grand public sans restriction légale d'accès ou d'utilisation. Ces informations sont mises à la disposition de tous les collaborateurs, avocats, individus ou entités externes au cabinet

Niveau 1 : Information «restreinte »

• Il s'agit du niveau par défaut quand aucune classification explicite n'est mentionnée.

- Les informations « restreintes » doivent être protégées, pour des considérations de propriété, d'éthique ou de respect de la vie privée, contre tout accès non autorisé.
- L'accès à ces informations n'est autorisé qu'aux collaborateurs ou aux personnes missionnées par le cabinet.

Niveau 2 : Information « confidentielle »

- Les informations confidentielles désignent toute information dont la divulgation auprès de personnes non autorisées ou dont l'utilisation inadéquate ou non autorisée est de nature à nuire à la capacité des entités opérationnelles ou à provoquer des évènements particulièrement dommageables affectant le SI du cabinet ou l'un de ses partenaires.
- Il en est de même pour toute donnée à caractère personnel hébergée ou gérée par le SI du cabinet

Quelques exemples d'informations confidentielles :

- Affectation des accès logiques,
- Affectation des authentifications (DIGIPASS, mots de passe, code PIN, certificat etc.), ou toute information concernant les flux donnant lieu à une authentification,
- Toutes les informations des clients du cabinet Nom, Prénom, Adresse, Numéro d'identité, Contrat, Etc.,
- Les incidents et failles de sécurité

II. Environnement de sécurité physique

- Les locaux hébergeant des équipements vitaux pour le système d'information du cabinet doivent tenir compte des menaces de l'environnement proche, et prévoir des mesures de protection contre les pannes et les accidents (pannes électriques, incendies, dégâts des eaux, etc.),
- Tous les équipements de protection et de détection installés dans les salles et les baies hébergeant les composants du SI du cabinet doivent être régulièrement contrôlés,
- Tous les accès physiques aux baies réservées au cabinet, aux panneaux de raccordements, aux salles des câbles et aux différents équipements réseau doivent être étudiés, validés et tracés. Seul le personnel compétent habilité a le droit d'effectuer des actions de maintenance (réparations, dépannage),

III. Classification et interconnexion des réseaux

Chaque réseau du SI du cabinet doit être qualifié en fonction :

- Du contrôle exercé par les entités du cabinet: réseaux internes ou externes.

Réseaux internes

- Un réseau est qualifié d'interne si le cabinet exerce un contrôle total sur celui-ci (installation, configuration, administration et utilisation).

Réseaux externes

- Un réseau est qualifié d'externe si le cabinet n'exerce aucun contrôle, ou exerce un contrôle restreint uniquement sur celui-ci.

Zone démilitarisée (DMZ)

- Une zone démilitarisée est un réseau qui isole les réseaux internes des réseaux externes au moyen de firewall.

IV. Contrôle des accès réseau

- L'accès au réseau ou son utilisation doit être organisé à travers une procédure mise en place par l'administrateur réseau. L'octroi de l'autorisation d'accès à un réseau doit être effectué par écrit.

- Les réseaux et les informations véhiculées ne peuvent être utilisés que par une personne, des systèmes ou des applications habilités ;

- Chaque autorisation d'accès au réseau n'est valable que pour un délai limité uniquement. À l'issue de ce délai, un contrôle doit être effectué afin de déterminer si le droit d'accès doit être prorogé ou non.

Mots de passe (Source : note technique ANSSI)

R1	Utilisez des mots de passe différents pour vous authentifier auprès de systèmes distincts. En particulier, l'utilisation d'un même mot de passe pour sa messagerie professionnelle et pour sa messagerie personnelle est à proscrire impérativement.
R2	Choisissez un mot de passe qui n'est pas lié à votre identité (mot de passe composé d'un nom de société, d'une date de naissance, etc.).
R3	Ne demandez jamais à un tiers de créer pour vous un mot de passe.
R4	Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.
R5	Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles.
R6	Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible.
R7	Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.
R8	Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se "souviennent" pas des mots de passe choisis.

Gestion des comptes d'accès

- L'administration des comptes d'accès (affectation, modification, suppression) doit se faire uniquement à travers les circuits préalablement définis par le cabinet,
- Tous les utilisateurs doivent être en possession d'un identifiant unique destiné à leur utilisation personnelle afin de garantir la traçabilité. Les utilisateurs sont responsables de toutes les opérations exécutées à l'aide de leur identifiant.
- Les identifiants utilisateur doivent remplir les critères suivants :

  Être nominatifs

  Ne pas fournir d'indication explicite quant au niveau de privilège de l'utilisateur (par exemple, administrateur ou associé)

  Être personnels (le même identifiant utilisateur ne peut pas être utilisé par plusieurs personnes, même sur plusieurs systèmes informatiques).

V. Gestion de vulnérabilités

La fonction gestion de vulnérabilités est une activité dirigée par un groupe de travail spécifique qui a pour missions :

De coordonner, faciliter et entreprendre toutes les activités nécessaires relatives aux correctifs de sécurité.

D'assurer une veille permanente de toutes les menaces connues ou vulnérabilités qui auraient des répercussions importantes sur les différents composants du système d'information. Ce groupe peut être abonné aux listes de diffusion de CERT (*Computer Emergency Response Team)* et aux flux d'information constructeurs des différents composants du SI du cabinet (Microsoft, Oracle, Apple, Apache, etc.)

Effectuer un suivi permanent du parc informatique du cabinet.

- En général, tous les composants du SI du cabinet doivent disposer de la dernière version / mise à jour publiée par le constructeur.
- Les correctifs de sécurité ne doivent être téléchargés que depuis les sites/sources officiels des différents constructeurs ou ceux considérés comme « sûrs ».
- Seules les personnes habilitées par le cabinet (internes ou prestataires de services) sont autorisées à effectuer des balayages de sécurité afin d'identifier les failles de sécurité exploitables depuis l'Intranet ou l'Internet.

VI. Planification de la continuité d'activités

- Dans le souci de minimiser l'impact du dysfonctionnement d'un système et d'éviter les pertes de données, un plan de continuité d'activité et de reprise d'activité peut être défini conformément aux besoins métiers et à la criticité des services proposés par le système du cabinet.

- La continuité d'activité et la récupération après sinistre doivent faire l'objet d'un contrôle périodique à travers des exercices de restauration unitaires et globaux.

- Il convient d'effectuer périodiquement des sauvegardes des données et des systèmes.

- Les processus de sauvegarde doivent être validés par le cabinet et être conformes :

- Aux plans de continuité des activités (par exemple, en matière de fréquence des sauvegardes) ;

- Aux obligations légales, réglementaires et contractuelles ;

- Aux recommandations des constructeurs (conditions de stockage et de durée maximale de conservation).

- Les sauvegardes doivent être :

- Clairement et précisément étiquetées (par exemple, en mentionnant la date et l'heure de la sauvegarde, la source des données, le numéro unique d'indexation ou encore la classification) ;

- Vérifiées afin de garantir que les fichiers sauvegardés peuvent être restaurés ;

- Stockées sur un site distinct de celui des données initiales (site distant)

- Protégées au moyen de contrôles de sécurité, conformément à la classification des données initiales.

VII. Sécurité des smartphones et des terminaux mobiles

Recommandations accessibles sur http://www.securite-informatique.gouv.fr/gp_article712.html

- Désactivez les liaisons inutilisées (Bluetooth, infrarouge, wifi], ...) et les services inutiles ;

- Paramétrez le pare-feu et le navigateur de manière restrictive;

- Utilisez un compte sans droits **administrateur ;**

- Mettez à jour les logiciels (système d'exploitation, navigateur, anti-virus, pare-feu personnel, etc…) ;

- Désactivez l'exécution automatique des supports amovibles (CDROM, Clés USB) ;

- Désactivez les services de partage de fichiers et d'imprimantes

- Sur les ordinateurs portables, installez un logiciel qui assure le chiffrement de l'environnement complet de travail (disque dur, fichiers temporaires, fichier d'échange, mémoire), en privilégiant une solution intégrée à l'architecture système qui soit transparente pour l'utilisateur ;
- Sur les Smartphones, installez un logiciel assurant le chiffrement de l'intégralité du répertoire de contacts, de l'agenda et des messages. À défaut, activez la protection d'accès par code PIN ;
- Installez un logiciel d'effacement sécurisé des fichiers afin de pouvoir éventuellement supprimer toutes les données sensibles lors du déplacement ;
- Configurez le serveur et le client de messagerie pour que les transferts de messages soient chiffrés par les protocoles SSL et TLS.

VIII. Clé E-barreau

- La « clé » e-barreau délivrée par le barreau de Paris est personnelle.
- Elle permet d'authentifier la personne connectée de manière certaine, mais également d'en attester la qualité d'avocat.
- Deux éléments composent cette « clé » :

Le support, sous forme d'une clé USB particulière, dédiée à l'authentification forte.

Un certificat logiciel, stocké de manière sécurisée sur la clé.

- Elle donne accès à une multitude de services en ligne dont e-barreau (échange avec les juridictions, y compris la Cour d'appel), e-carpa (accès à vos comptes maniements de fonds en ligne, y compris les demandes de virements), mais aussi la possibilité d'utiliser la signature électronique, ou encore d'accéder aux téléservices mis à disposition par les administrations.
- Le certificat logiciel (sorte de carte d'identité numérique) contient deux informations importantes :

  L'identifiant CNBF de l'avocat,

  Un numéro SIREN.

- Afin de ne pas être dans l'obligation de générer une nouvelle clé en cas de changement de structure, nous renseignons de préférence le numéro SIREN de l'avocat et non celui de la structure d'exercice dans le certificat.

C. Quelques références

- **ANSSI**

Guide d'hygiène informatique.
http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

Partir en mission avec son téléphone mobile, son assistant personnel ou son ordinateur portable http://www.securite-informatique.gouv.fr/gp_article712.html

- **CENTRE D'ANALYSE STRATÉGIQUE**

Cybersécurité, l'urgence d'agir (Note d'analyse 324 - Mars 2013) http://www.strategie.gouv.fr/content/cybersecurite-urgence-na324

- **Le CERTA**

http://www.certa.ssi.gouv.fr/

- **CNIL**

Un nouveau guide pratique à destination des avocats. http://www.cnil.fr/la-cnil/actu-cnil/article/article/un-nouveau-guide-pratique-a-destination-des-avocats/

- **Conseil National des Barreaux**

Sécurité de l'information au sein des cabinets - deux guides mis à disposition de la profession. http://cnb.avocat.fr/Securite-de-l-information-au-sein-des-cabinets-deux-guides-mis-a-disposition-de-la-Profession_a1191.html

- **VERIZON**

Rapport d'enquête 2013 sur la compromissions des données (rapport DBIR)

http://www.verizonenterprise.com/resources/reports/es-rapport-d'enquete-2013-sur-les-compromissions-de-donnees 20_fr_xg.pdf

- **SYMANTEC**

Annual threat report (16 avril 2013). http://www.symantec.com/security_response/publications/threatreport.jsp