ORDRE DES AVOCATS DE PARIS

VADE MECUM DE LA DEONTOLOGIE DU NUMERIQUE

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

:01

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.