VADEMECUM DES OUTILS NUMERIQUES DE L'AVOCAT

Conseiller et défendre en toute confidentialité

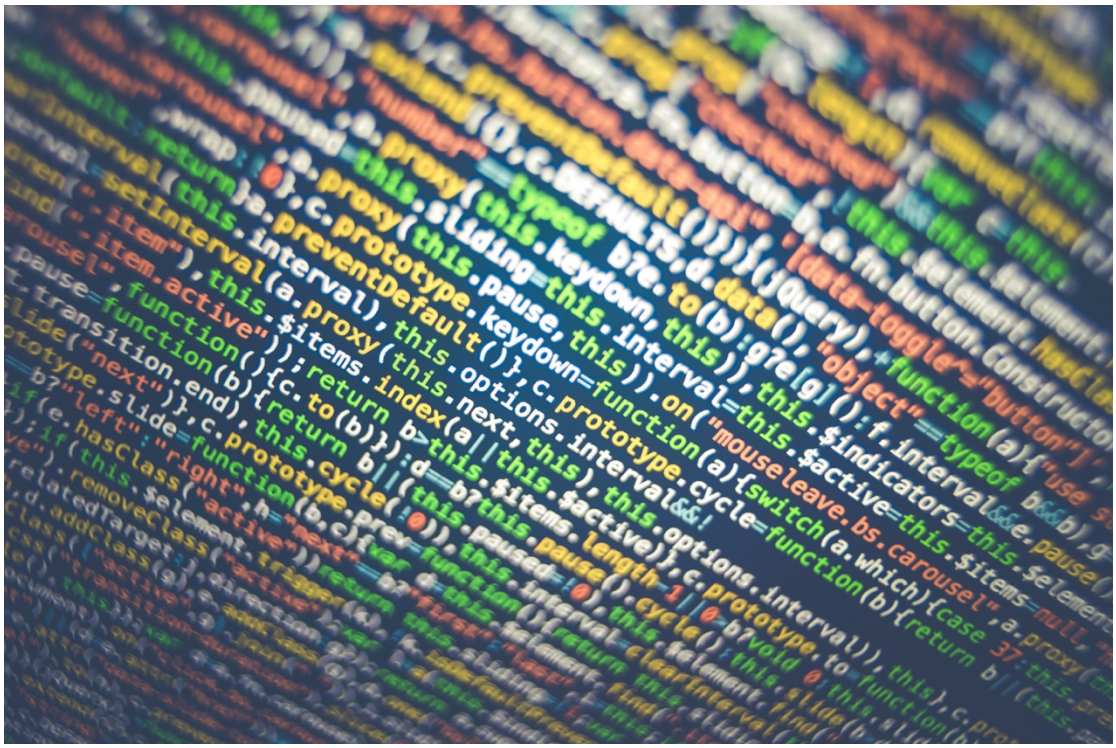

Image Markus Spiske

Commission Numérique du SAF/Octobre 2023

SAF

SYNDICAT DES AVOCATS DE FRANCE

TABLE DES MATIERES

AVANT-PROPOS

Ou l'intérêt d'utiliser des outils avec une haute exigence de confidentialité

L'avocat est par essence le détenteur des secrets de ses clients, ce qui est le socle de son intervention et de sa légitimité. Secret professionnel, secret de l'enquête et de l'instruction, secret des correspondances ; voici des notions que nous maîtrisons parfaitement. Notre cabinet est un sanctuaire. Mais à l'heure du smartphone, du cloud, des mails et des échanges numériques devenus la règle et le papier l'exception, beaucoup d'entre nous avons pris le train technologique en marche sans s'interroger de la confidentialité absolue des outils utilisés.

Force est de constater que beaucoup d'outils, en particulier ceux proposés par les GAFAM, ne satisfont aucune exigence de confidentialité. En effet, ***toute solution US sera soumise ~~et~~ à la législation étatsunienne comprenant Cloud Act et Patriot Act imposant un accès aux instances fédérales des données traitées par leurs firmes***. Le Cloud Act et le Patriot Act permettent aux autorités américaines de récupérer les données d'une personne, y compris si celle-ci est de nationalité étrangère, et y compris si les données sont stockées sur un territoire étranger par une société américaine.

Dès lors, utiliser les outils comme Google, Icloud, un cloud Amazon, ou encore Microsoft Office 365 ne vous garantit pas la confidentialité exigée par le RIN (Art. 66-5 du décret 71-1130 et Art. 4 du décret n°2005-790), le code pénal (Art. 226-13) ou encore la Loi Informatique et Liberté et le RGPD.

En effet, Respecter le secret professionnel implique de ne pas utiliser des services qui ne garantissent pas la confidentialité des données.

Bonne nouvelle, il existe des solutions simples et souvent gratuites qui vous garantissent un haut niveau de confidentialité si vous ne souhaitez pas investir dans des solutions proposées par les éditeurs, qui ne sont d'ailleurs pas toujours complètes ni conformes à la

législation. Nous vous proposons dans ce présent vademecum des outils disponibles.

Ce vademecum s'adresse essentiellement à des confrères exerçant de manière individuelle, et a pour ambition de partager des solutions simples et pratiques assurant un niveau de confidentialité élevé dans leur exercice professionnel.

1. LA COMMUNICATION ELECTRONIQUE

Nous utilisons des emails au quotidien, mais aussi des SMS, et des applications de messagerie, ou encore des solutions de transfert de données ou des documents partagés.

A. Email : si c'est gratuit, c'est toi le produit !

Cette citation, pas tout à fait exacte, a le mérite d'interpeller sur les messageries et suites qui vous sont proposées gratuitement. Nombre d'entre nous utilisent les messageries Gmail, Hotmail, ou autre solution qui ne garantissent pas le niveau de sécurité exigé par notre profession. Outre le Cloud Act et le Patriot Act, votre fournisseur de messagerie accède à vos messages pour vous proposer des publicités ciblées… A noter que le Parlement Européen, dans le cadre de la lutte contre les abus sexuels des enfants (CSAR), étudie l'obligation pour les fournisseurs de messagerie de scanner les messages et photos de leurs clients….

° Solutions chiffrées de bout en bout :

Ces services vous garantissent que seul les possesseurs de la clef privée de déchiffrement peuvent accéder aux mails et aux infos qu'ils contiennent.

Ces solutions très sures imposent cependant des contraintes d'utilisation fortes puisque vous ne pouvez vous y connecter qu'en fournissant votre clef personnelle chiffrée. Si vous la perdez, personne ne pourra réinitialiser vos accès et vous devrez utiliser des clients logiciels spécifiques fournis par le prestataire.

- les principaux fournisseurs en 2024 :

Protonmail - Tuta (anciennement Tutanota) - Posteo – Mailbox.org

° Solution non chiffrées

Les prestataires fournissent des solutions permettant l'intéropérabilité IMAP/POP/SMTP permettant d'intégrer leurs solutions avec les logiciels clients mails classiques (Thunderbird, Outlook, Evolution…) et les différents appareils (smartphone, tablettes, pc, portables).

Il faut bien vérifier la compatibilité RGPD de leurs conditions générales et la localisation des données, car le prestataire a, par construction technique, accès à l'ensemble des mails qui transitent sur ses serveurs.

Les services gratuits ont, généralement, pour contrepartie le traitement de vos données pour revente à des tiers. Leurs conditions d'utilisation sont toujours contraires aux obligations déontologiques pour une utilisation professionnelle.

Vous pouvez également chiffrer les messages échangés (avec OpenPGP) mais seuls le corps des messages sera chiffré et votre interlocuteur devra savoir gérer les échanges de clefs privées/publiques.

OVH vous propose un service d'email qui vous permet de disposer d'un email couplé avec votre propre nom de domaine. Hébergé en France, OVH est soumis à la législation française et garantit donc un niveau de confidentialité satisfaisant de base et vous pouvez opter pour des certifications de sécurité plus exigeantes comme SecnumCloud ou HealthDataHub (certification données de santé), mais le cout est très élevé et ne se limite pas aux mails mais à un ensemble de services de traitements numériques.

B. Le smartphone

Au-delà des recommandations de sécurité que l'on peut trouver sur le site de l'ANSSI, l'utilisation de votre smartphone peut être optimisée en matière de sécurité.

Paramétrage de votre téléphone afin d'éviter tout partage d'information avec les fabricants (tous les téléphones du marché disposent de composants opaques pouvant permettre la transmission de vos données à des tiers, de nombreuses utilisations de ces composants opaques ont déjà été observés vers des constructeurs ou des Etats) : Nous rappellerons ici que d'origine, de nombreuses données tapées sur le clavier de votre téléphone sont envoyées à leur fabricant. Des claviers virtuels respectueux de votre vie privée (mais beaucoup moins intuitifs -on ne peut pas tout avoir-) sont disponibles en téléchargement.

Vous pouvez aussi installer des systèmes d'exploitation permettant de ne pas vous obliger à lier votre utilisation à Apple (compte Icloud) ou Google (compte Gmail) comme *eOs* ou Lineage

Utilisation des messageries cryptées WhatsApp, Signal, Telegram, Facebook Messenger : Nous utilisons tous des applications de messagerie sur nos téléphones, et de plus en plus en usage professionnel. WhatsApp et Facebook Messenger étant géré par Meta, anciennement Facebook, le Cloud Act et le Patriot Act s'y appliquent.

Privilégiez donc les applications totalement confidentielles dès lors que vous communiquez avec vos clients, préférez donc Signal à Whatsapp et définissez des durées de conservation des messages.

Pour les visioconférences, préférez les solutions libres comme Jitsi à leurs équivalents propriétaires (Zoom, Teams…) dont rien ne garantit vraiment ni la confidentialité, ni la sécurité.

Utilisation d'application de navigation : Là encore, les applications classiques type Google ou Bing sont peu respectueuses de votre vie privée. Or, les navigateurs Firefox ou Brave garantissent un niveau de sécurité plus important, sur l'ensemble de vos outils numériques par l'ouverture de leur code et leur respect des normes intéropérables W3C.

C. Recherche sur internet

Les recherches sur internet peuvent mettre en danger la confidentialité des informations que contiennent vos requêtes ou permettre au site de recherche de collecter vos sujets de recherches.

L'utilisation de moteurs de recherche ne procédant pas à la collecte systématique de vos requêtes (comme les services Google) permet d'éviter ce risque : DuckDuckGo / Startpage

D. Mots de passe et chiffrement

La CNIL a édité des recommandations concernant les mots de passe, qu'ils soient situés sur vos smartphones ou vos autres périphériques.

Quelques conseils de base (Merci Antoine BON) :

Ne jamais utiliser un même mot de passe sur plusieurs sites

- Une faille de sécurité sur un seul site compromettrait tous vos accès !
- Les pirates utilisent des robots qui testent les mots de passe volés sur les sites populaires

Ne notez pas vos mots de passe sur des post-it ou dans votre téléphone

- Ne notez jamais un mot de passe en clair
- Utilisez des logiciels de gestion de mot de passe (intégré à votre navigateur Firefox ou mieux encore auto-hébergé dans un endroit sûr (KEEPASS)

N’envoyez pas vos mots de passe par courriel

- Votre boite mail est la première cible des pirates
- Des logiciels scannent les boites mails à la recherche de mots de passe

N’utilisez pas aveuglément la fonction « enregistrer votre mot de passe »

• Vous ne faites que reporter le risque sur le mot de passe de votre ordinateur ou de votre navigateur.

Activer l’authentification à deux facteurs (2FA) quand elle est disponible

- Évitez la validation par SMS
- Privilégiez les codes autogénérés (2FAS, AUTHY)

Modifiez toujours les mots de passe enregistrés par défaut

- Surtout sur les box internet, routeurs et autres équipements réseau
- Évitez les identifiants évidents : admin / user / root

Le plus pratique étant d’utiliser un gestionnaire de mots de passe sur l’ensemble de vos outils, qui vous permet de ne retenir qu’un seul mot de passe. Les solutions libres ne sont pas toujours très intuitives et des solutions payantes, disponibles sur les app stores, sont parfois un bon investissement. Datavault est une solution qui fonctionne bien et qui ne nécessite qu’un seul achat et aucun abonnement…

2. LE STOCKAGE NUMERIQUE

Là encore, la pratique s’est développée de façon empirique pour beaucoup de confrères qui n’ont pas véritablement pensé leur stockage et se retrouvent sans une solution sure.

A. Sauvegarder

Sauvegarder vos données est une obligation tant déontologique que légale. En effet, le RIN et le RGPD vous imposent de conserver les données dont vous disposez dans vos dossiers.

Les questions plus techniques sur les durées de conservation, l'information de vos clients etc… ne seront pas traitées ici.

Retenons qu'au-delà d'une pratique nécessaire à notre bon exercice professionnel, sauvegarder nos données est **indispensable**.

Comment faire ?

Si vous ne disposez que d'un terminal (un pc portable ou fixe), vous pouvez utiliser un disque dur externe et faire vos sauvegardes régulièrement. Attention à votre régularité et à la sécurité de cette sauvegarde : chiffrez-là et conservez-là dans un endroit sécurisé.

Des installations plus complexes de NAS (un disque dur branché sur votre réseau interne et faisant des sauvegardes automatiques) nécessitent des compétences plus abouties ou l'intervention d'un prestataire et peut également être une solution adéquate.

Si vous disposez de plusieurs terminaux, l'idéal est de stocker vos dossiers en cloud.

Les solutions étasuniennes Icloud, Google, Amazon ou Microsoft sont donc à proscrire toujours et encore du fait du Cloud Act et du Patriot Act.

Plusieurs solutions vous sont proposées.

Le CNB propose une solution de cloud qui évolue au 31 décembre prochain qui permet un stockage et une solution de partage qui s'adaptera à de nombreux confrères que l'on trouve dans l'espace sécurisé du CNB.

D'autres prestataires comme WIMI, TRANSFERTPRO, 100% français, ou d'autres vous proposent des solutions allant du drive au transfert de fichiers et agenda permettant d'assurer la confidentialité. Votre environnement de travail se trouve peu modifié sur votre ordinateur,

avec des dossiers apparaissant sur votre ordinateur en mode hors ligne et une synchronisation dès l'accès à internet.

Il s'agit généralement de solutions configurées à partir de logiciels libres comme Nextcloud que vous pouvez également déployer directement sur vos infrastructures si vous savez le faire de manière sécurisée.

B. Transmettre

La transmission de données est un vrai sujet en matière de confidentialité et de RGPD. En effet, **les données sensibles ne doivent pas transiter par mail,** afin d'éviter la faille de sécurité la plus commune que représente l'erreur d'adressage. En pratique, cette règle est souvent inappliquée tant par les juridictions que par les confrères. Pourtant, les solutions ne manquent pas.

Échange avec les clients : *Le courrier papier* est devenu l'exception. Il reste pourtant un mode de communication réputé confidentiel. Des solutions de *chiffrements de fichiers* existent et peuvent être utiles pour les confrères mais le système peut paraître rapidement inadapté compte tenu du nombre d'emails envoyés et de données traitées. Plus simple pour le confrère qui dispose d'une solution d'hébergement en cloud, la possibilité de créer un dossier spécifique pour que le client y verse ses éléments, soit par le biais d'un lien sécurisé, soit par le biais de la création d'un espace sécurisé.

Échange avec les juridictions **:** La encore, l'échange d'écritures et de pièces par email est à proscrire. En matière pénale, PLEX vous permet à la fois de recevoir des fichiers mais également de les adresser aux juridictions. En matière civile, le RPVA permet, avec ses limites, de partager des fichiers avec les juridictions. En matière administrative, Télérecours est d'ores et déjà bien connu des confères et de l'avis de tous, fonctionne bien.

Échange avec les confrères : Comme pour vos clients, les échanges avec les confrères peuvent s'effectuer par lien de téléchargement, que vous avec la possibilité de crypter. Le CNB a édité un service e-partage, basé sur la solution libre

C. Collaborer en ligne

Difficile de se passer de Google ? vous connaissez certainement Framasoft, une association qui édite des applications totalement libres, sans publicité et respectueuses qui vous permet de vous passer des outils collaboratifs de Google.

Simple et gratuit, c'est une solution qui vous permet d'utiliser des outils de communication, de sondage et d'agenda qui sont compatibles avec vos ordinateurs et smartphones.

3. POUR ALLER PLUS LOIN : OPTIMUS AVOCATS, UNE SUITE D'OUTILS DE CABINET

Des solutions payantes existent sur le marché permettant une interopérabilité entre les différents outils.

Néanmoins, des confrères passionnés de logiciels libres (dont un membre de la commission numérique) ont développé une solution de gestion de cabinet assez complète et totalement gratuite permettant de produire, stocker, transmettre et gérer votre cabinet.

Attention toutefois à vous faire accompagner pour mettre en place cette solution, qui peut paraître ardue pour les béotiens. Après deux tentatives seul, le rédacteur de ces lignes a du solliciter l'intervention d'un expert pour l'accompagner ;)