Stämpfli
Verlag

Anwaltsrevue|Revue de l'avocat 4/2022 |S. 179–184 179

Anwaltspraxis

LES COMMUNICATIONS NUMÉRIQUES DE L'AVOCAT AVEC SON CLIENT: QUELS OUTILS EN 2022?

Alexandre Jotterand Avocat, CIPP/E, CIPM, id est avocats Sarl

Mots-clés: communication, outils numériques, secret professionnel, protection des données

L'avocat doit exercer sa profession dans le respect du secret professionnel et des règles sur la protection des données, tout en étant réactif et efficient. Confronté à ces exigences, il doit déterminer quels outils numériques il peut utiliser pour communiquer avec ses clients et quelles sont les précautions à prendre. Cet article analyse les risques liés aux divers modes de communication et fournit des recommandations sur leur utilisation.

I. Introduction

À l'heure où les mesures d'urgence liées au COVID s'amenuisent et que les salles de réunion se remplissent à nouveau, il apparaît opportun de dresser un point de situation concernant les modes de communication entre l'avocat[1] et son client.

Après un bref rappel des principes applicables (*infra,* II.), nous présenterons et comparerons différents outils (numériques ou non)[2] (*infra,* III.) et émettrons certaines recommandations (*infra,* IV.).

II. Principes généraux

1. Toute communication implique des risques

Toute communication implique des risques. Ces risques vont varier – tant dans leur probabilité que dans leur gravité potentielle – en fonction de plusieurs facteurs, tels que le moyen de communication employé, la sensibilité des informations échangées (informations «banales», secrets hautement confidentiels, informations médicales), ainsi que de la probabilité que ces informations puissent intéresser des tiers[3].

Le risque principal – et commun – à tous les moyens de communication est celui d'un *accès à tout ou partie de la communication par un tiers non autorisé* (atteinte à la confidentialité du message)[4], dont résulterait une violation du secret professionnel[5]. À ce danger s'ajoute le risque d'une violation des droits de la personnalité en cas de traitement violant les règles sur la protection des données[6]. Dans les deux cas, il convient de distinguer l'accès aux informations relevant du *contenu de la communication* de celles se rapportant *à la communication elle-même,* soit les métadonnées (p.ex. identité et adresse de l'émetteur et du destinataire, date d'envoi, fréquence des appels, etc.).

Sur la base des risques identifiés, l'avocat devra décider avec son client (*infra,* II.2.) des moyens de communication appropriés et des mesures de sécurité à mettre en place. La nécessité de limiter les risques devra être mise en balance avec les inconvénients qu'engendre immanquablement toute mesure de sécurité supplémentaire, notamment en termes de difficulté d'implémentation et de coûts de mise en œuvre, ains que des possibles complications pratiques pour les activités du client et de l'avocat (comme par exemple celle de changer fréquemment de système).

2. Le (choix du) client est roi

Comme exposé ci-après, ni les règles sur le secret professionnel, ni celles découlant de la LPD ne s'opposent au recours à des moyens de communication numériques.

C'est principalement la volonté du client et son appétence au risque explicite ou présumée qui dicteront le choix des outils de communication appropriés. Il importe donc d'obtenir l'accord du client sur ce point dès la conclusion du mandat. Cet accord peut toutefois intervenir de manière tacite et résulter des circonstances[7], ce qui sera le cas si le client initie la conversation ou ne réagit pas au moyen de communication employé par l'avocat.

À notre avis, ce n'est que dans des circonstances particulières que l'avocat pourrait être tenu de rendre son client attentif aux risques spécifiques de sécurité pour les données[8].

3. Le secret professionnel

L'art. 13 LLCA interdit la divulgation du secret confié par le client et oblige l'avocat à prendre les précautions nécessaires pour sa conservation, y compris dans l'usage des moyens de communication. Le souci de garantir le secret professionnel est l'un des devoirs d'une conduite professionnelle prudente et consciencieuse au sens de l'art. 12 let. a LLCA[9].

En lien avec les devoirs de l'avocat découlant de la LLCA, l'utilisation d'outils numériques de communication pose essentiellement les mêmes questions que le recours au *cloud.* Tant l'envoi d'e-mails, que l'utilisation de messageries instantanées ou de systèmes de visioconférence impliqueront en effet généralement l'accès par le fournisseur, qui pourra se situer aussi bien en Suisse ou à l'étranger, à des informations couvertes par le secret professionnel (chiffrées ou non). Nous renvoyons aux nombreux articles récents qui ont déjà abordé cette question[10] et rappellerons uniquement que:

- Il n'y a pas de divulgation du secret professionnel si les données sont chiffrées et que le fournisseur de services ne dispose pas de la clé nécessaire à leur déchiffrement[11].
- Le secret professionnel ne s'oppose pas à la transmission d'informations non chiffrées à un fournisseur de services, car celui-ci doit être considéré comme un auxiliaire de l'avocat au sens de l'art. 321 al. 1 CP[12].
- Ce principe vaut également si le fournisseur a son siège, ses serveurs ou ses employés à l'étranger. Une analyse des risques doit toutefois être effectuée dans ce cas, notamment quant au risque d'accès aux informations par des autorités étrangères[13].
- S'il recourt à un auxiliaire, l'avocat doit le choisir soigneusement et veiller à ce qu'il respecte le secret professionnel[14].

4. La protection des données

L'avocat suisse est soumis à la loi fédérale sur la protection des données (LPD)[15], dont la version révisée devrait entrer en vigueur en septembre 2023 (ci-après «nLPD»)[16]. Les principes suivants sont pertinents en lien avec la présente problématique:

La communication de données personnelles à un sous-traitant ne nécessite ni le consentement des personnes concernées, ni un autre motif justificatif, pour autant que les dispositions de l'art. 10*a* LPD (9 nLPD) soient respectées[17]. En particulier, *aucune obligation légale ou contractuelle de garder le secret* ne doit s'opposer à la sous-traitance. En règle générale, cette condition sera respectée puisque le secret professionnel ne s'oppose pas à la communication de données à un fournisseur de services de communication (même sous une forme non chiffrée)[18]. Il reste toutefois concevable que le contrat avec le client prévoie une obligation de confidentialité qui s'oppose à une telle externalisation[19].

En cas d'accès aux données personnelles depuis l'étranger (notamment en raison du lieu de stockage des données ou du lieu où se trouvent les employés du fournisseur qui auront accès à distance aux données), les dispositions de l'art. 6 LPD (16 à 18 nLPD) devront être respectées. Le transfert de données vers les pays de l'Union européenne ou les (rares) autres pays reconnus comme assurant un niveau de protection adéquat en matière de protection des données est possible sans autre restriction. La communication de données vers tous les autres pays, y compris les États-Unis, nécessite la mise en place de garanties appropriées. Dans ce cas, l'exportateur des données doit s'assurer que le transfert soit encadré non seulement par les dispositions contractuelles nécessaires, mais également par des mesures techniques et organisationnelles appropriées[20]. En pratique, ces questions sont complexes et requièrent une analyse détaillée en lien avec

le transfert envisagé. À noter que l'Union européenne et les États-Unis ont récemment annoncé avoir trouvé un nouvel accord visant à simplifier les transferts transatlantiques de données personnelles, lequel doit encore être formalisé[21].

Enfin, le nouveau droit suisse de la protection des données renforcera l'obligation d'informer les personnes concernées, y compris quant aux (catégories de) destinataires des données, ainsi qu'aux pays dans lesquels celle-ci pourront être accessibles (art. 19 al. 2 let. c et al. 4 nLPD)[22]. Il s'agit d'un élément important, puisque le manquement intentionnel aux obligations d'informer pourra tomber sous le coup de dispositions pénales (art 60 al. 1 let. b ch. 1 nLPD).

III. Outils (numériques ou non) à disposition de l'avocat

1. Les moyens de communication «traditionnels»

Comme évoqué ci-avant (*supra,* II.1.), tous les moyens de communication impliquent des risques, qui n'épargnent pas les outils «classiques» que sont le courrier et le téléphone. C'est par rapport à ces risques généraux qu'il convient d'analyser l'opportunité de recourir à des outils numériques de communication.

Premièrement, le courrier et le téléphone peuvent faire l'objet de mesures de surveillance, y compris rétroactives[23], ordonnées par une autorité. La protection offerte par le secret de l'avocat connaît des limites: elle ne s'appliquera *a priori* qu'en Suisse et uniquement pour les activités typiques de l'avocat. Dans les autres cas,

notamment dans le contexte de communications à l'étranger, il n'est pas exclu qu'un outil numérique offrant une meilleure protection soit à privilégier.

Deuxièmement, le courrier peut être réceptionné et/ou ouvert par un tiers autre que son destinataire. En dehors du cas du courrier relatif à des conseils matrimoniaux réceptionné par l'autre époux, cette problématique doit faire l'objet d'une attention particulière lorsque le client est une personne morale. En effet, l'avocat ne doit communiquer qu'avec ses interlocuteurs autorisés, soit les individus désignés comme tels par la société. Suivant les circonstances, l'envoi d'un e-mail à l'attention d'un destinataire pourvu d'une boîte e-mail nominative offrira davantage de sécurité que celui d'un courrier, qui pourrait passer entre de nombreuses mains avant d'atteindre son destinataire[24].

2. La télécopie

La télécopie souffre de manière générale des mêmes risques que le courrier, soit en particulier celui qu'une fois réceptionnée, son contenu soit lu par des personnes qui n'en sont pas les destinataires[25]. Au demeurant, le fax est généralement moins sûr qu'un e-mail: les télécopieurs communiquent en effet sur les lignes téléphoniques sans aucun chiffrement[26]. Pour ces raisons, nous recommandons de le proscrire au profit d'autres moyens de communication.

3. Les e-mails

L'e-mail a mauvaise presse. On dit de lui qu'il est l'équivalent en matière de sécurité de l'envoi d'une carte postale sans enveloppe[27]. Certains auteurs estiment même que le fait pour les avocats d'envoyer à leurs clients des e-mails non chiffrés constituerait une faute professionnelle[28]. La réalité est toutefois plus complexe.

Sur le plan technique d'abord, les e-mails sont souvent mieux sécurisés qu'on ne le pense (*infra,* III.3.A). Ensuite, la nécessité de mesures de sécurité additionnelles doit être évaluée en fonction du risque effectif (*supra,* II.1.) et de l'appétence du client au risque (*supra,* II.2.).

A) Chiffrement par défaut des e-mails (TLS)

Dans la grande majorité des cas, les e-mails sont sécurisés par défaut conformément au protocole TLS *(Transport Layer Security),* qui chiffre leur contenu lors de leur transmission, sans qu'un réglage par l'avocat ou son client soit nécessaire. Ce protocole a pour vocation de rendre impossible (ou à tout le moins plus difficile, puisque rien n'est impossible en matière de sécurité) la lecture du contenu de l'e-mail durant sa transmission. Il protège notamment contre la surveillance des réseaux par des autorités de surveillance[29], ou l'accès par des tiers mal intentionnés. Le contenu du message pourra cependant être déchiffré par le fournisseur de service lorsqu'il transite ou est stocké sur ses serveurs[30]. Ce dernier point différencie le chiffrement TLS du chiffrement de bout en bout (*infra,* III.3.C).

Pour que le protocole TLS puisse s'appliquer, il faut que les fournisseurs de messagerie de l'expéditeur et du destinataire l'utilisent tous les deux, ce qui est le cas aujourd'hui de la majeure partie d'entre eux, dont Google et

Microsoft[31]. À noter que si le courriel n'est pas protégé par TLS, l'utilisateur n'en sera pas nécessairement informé au moment d'envoyer son message[32].

L'avocat doit s'assurer que sa messagerie supporte la norme TLS et qu'il pourra recevoir et envoyer des e-mails chiffrés de bout en bout si le client le désire. Sous cette réserve et en règle générale, l'envoi d'e-mails «standards» (qui ne sont donc pas chiffrés de bout en bout) est une méthode acceptable de communication entre l'avocat et son client.[33]

B) La signature des e-mails

La signature des e-mails permet d'assurer que l'identité de l'expéditeur n'est pas usurpée. Elle ne protège donc pas la confidentialité, mais l'intégrité de la communication. Elle nécessite l'obtention d'un certificat personnel émis par une autorité de certification, auprès de laquelle il devra être acquis. À noter qu'une fois obtenu, le certificat permet également la réception d'e-mails chiffrés selon le protocole S/MIME (*infra,* III.3.C). Relativement simple et peu coûteuse à mettre en place, cette mesure devrait à notre avis être adoptée par tout avocat utilisant les e-mails comme moyen de communication.

C) Chiffrement de bout en bout (E2E Encryption)

Avec un chiffrement de bout en bout *(end-to-end encryption* ou *E2E),* le contenu d'un e-mail ne peut être déchiffré que par son destinataire. Le fournisseur de service ne peut pas le lire, ni a fortiori le transmettre à des autorités suisses ou étrangères.

Ce chiffrement considéré comme «fort» repose le plus souvent sur le protocole S/MIME *(Secure Multipurpose Internet Mail Extensions)*[34]*,* qui nécessite que l'expéditeur et le destinataire disposent tous deux (i) d'une application de messagerie prenant en charge la norme S/MIME, et (ii) d'un certificat personnel émis par une autorité de certification (identique à celui émis pour la signature des e-mails).

Un constat: cette technologie, qui n'est pas nouvelle, ne s'est jamais imposée malgré ses avantages indéniables en matière de sécurité. La raison principale réside dans le fait que tant l'expéditeur que le destinataire doivent disposer de systèmes «compatibles»[35], dans un monde où chacun reçoit et envoie des dizaines (voire des centaines) d'e-mails par jour à de nombreux correspondants. Le chiffrement de bout en bout paraît donc peu approprié à la correspondance quotidienne et usuelle effectuée par e-mail.

En revanche, il appartient à l'avocat de s'assurer de pouvoir communiquer de cette manière si son client en fait la demande, ou si des circonstances spéciales l'exigent.

L'avocat qui recourt au chiffrement de bout en bout doit être conscient de certains inconvénients. Premièrement, seul le *contenu* de l'e-mail sera chiffré et non ses métadonnées (ce qui comprend non seulement les informations sur l'expéditeur et les destinataires du message, mais également le texte en objet)[36]. Ensuite, le chiffrement de bout en bout va également chiffrer les éventuels logiciels malveillants qui seraient contenus dans l'e-mail, ce qui risque d'empêcher leur détection et de participer à leur propagation[37]. Enfin, l'avocat devra veiller à archiver les certificats nécessaires au déchiffrement (ceux-ci pouvant changer au fil du temps) en même temps que les e-mails, sans quoi il pourrait perdre tout accès aux e-mails archivés[38].

D) Les messageries sécurisées

Au-delà de la technologie S/MIME (qui s'intègre dans la messagerie de l'avocat), certains fournisseurs offrent des systèmes permettant d'envoyer *par défaut* des e-mails chiffrés de bout en bout. Tel est le cas de ProtonMail. Il faut toutefois que le destinataire utilise également cette messagerie. Dans les autres cas, la mise en place d'un chiffrement de bout en bout nécessite des démarches complexes[39]. L'utilisation d'une messagerie de type ProtonMail reste marginale en pratique, et l'avocat risque de ne l'utiliser qu'en lien avec certains mandats spécifiques. Ceci

nécessiterait qu'il surveille plusieurs boîtes mails, ce qui peut poser d'autres problèmes, notamment en matière de réactivité.

4. Les services de visioconférence

A) Introduction

Durant les périodes de restrictions liées au COVID, la visioconférence est devenue le moyen de communication privilégié.

À condition d'utiliser les services d'un prestataire réputé, la visioconférence offre en règle générale un niveau de sécurité plus élevé que la communication par e-mail (dans une configuration standard), voire même que le téléphone ou le courrier (dans certains cas de communication transfrontière). Il n'en demeure pas moins que la majorité des fournisseurs ont leur siège aux États-Unis, ce qui génère des risques en matière de maintien du secret professionnel et de conformité à la LPD[40].

Une analyse détaillée des différents services offerts en lien avec le respect de la protection des données et de la confidentialité dépasserait le cadre de la présente contribution. Nous renvoyons à l'analyse comparative du préposé à la protection des données du canton de Zurich[41], ainsi qu'à la comparaison effectuée par l'ONG noyb.eu des politiques de confidentialité de différents fournisseurs[42]. Nous nous contenterons de mettre en exergue certains points importants.

B) Zoom

Zoom offre par défaut un chiffrement des données en transit (notamment par le protocole TLS) et de bout en bout, offrant ainsi un niveau de sécurité élevé contre l'accès aux contenus des conversations tant par les employés de Zoom que par des autorités[43]. Ceci ne s'applique toutefois pas aux métadonnées collectées par ce service.

C) Microsoft Teams

La licéité du recours aux services de Microsoft a été récemment discutée dans la présente revue[44]. Microsoft Teams utilise le protocole TLS pour chiffrer les données en transit, et déploie également un chiffrement de bout en bout, pour le moment toutefois uniquement en lien avec les appels individuels non programmés[45]. Au demeurant, les utilisateurs de ce service peuvent limiter via certains réglages l'accès par Microsoft aux contenus relatifs aux conversations éventuellement enregistrées, tels que les messages envoyés par *chat* ou la transcription des appels[46].

D) CISCO WebEx

CISCO WebEx offre également un chiffrement de bout en bout. Son utilisation par la Cour de Justice de l'Union européenne a été validée par le Contrôleur européen de la protection des données[47].

E) Jitsi

Jitsi est un service de visioconférence européen et dont le code est en libre accès. Il est possible de le configurer

pour bénéficier d'un chiffrement de bout en bout, à condition toutefois d'utiliser Jitsi dans un navigateur compatible[48].

5. Messageries instantanées

Enfin, les avocats peuvent communiquer avec leurs clients par messages instantanés, que ce soit par WhatsApp, Signal, ou d'autres services.

L'utilisation de WhatsApp, Threema, Signal, Telegram ou iMessage (service d'Apple) pose fondamentalement les mêmes questions et offre les mêmes garanties que l'utilisation de systèmes de visioconférence. Le lecteur trouvera sur Internet de nombreuses analyses et comparaisons relatives à ces différents outils[49].

Nous nous contenterons de relever que WhatsApp, Threema, Signal et iMessage offrent toutes un chiffrement de bout en bout. Ce n'est toutefois pas le cas de l'application Telegram. À l'exception de celle-ci, les messages envoyés avec ces solutions sont donc plus sécurisés que les communications effectuées via e-mail, SMS ou téléphone: aucune des sociétés exploitant ces solutions ni aucune autorité ne pourront accéder aux contenus échangés. En revanche, il existe des différences concernant les modalités de collecte des métadonnées ou autres données secondaires, terrain sur lequel Threema est meilleur que ses concurrents et WhatsApp fait figure de lanterne rouge.

En définitive, ni le secret professionnel, ni les règles sur la protection des données n'interdisent fondamentalement à l'avocat de communiquer avec son client au moyen d'un service de messagerie instantanée, y compris WhatsApp, hormis dans des situations particulières où l'exploitation des données secondaires (métadonnées) comporterait des risques spécifiques[50].

IV. Recommandations

Sur la base de ce qui précède, nous formulons les recommandations suivantes en lien avec l'utilisation d'outils de communication numériques par l'avocat:

- Informer son mandant de son rôle dans le choix des moyens de communication et des mesures de sécurité nécessaires, et des éventuelles complications pratiques qu'elles impliquent.
- S'assurer que sa messagerie électronique supporte le protocole TLS et signer systématiquement tout e-mail selon la norme S/MIME. Si l'on ne peut attendre de l'avocat qu'il chiffre impérativement de bout en bout et par défaut chaque e-mail qu'il envoie, il doit être en mesure de le faire si son client en fait la demande ou si un risque particulièrement élevé l'impose.
- Adapter les mesures de sécurité en présence de risques particuliers[51] (qu'il faut donc comprendre et anticiper), ou lorsque le client en fait la demande.
- Faire mention du caractère secret de la communication.
- En cas de recours à des services de visioconférence ou de messagerie instantanée, choisir les fournisseurs avec soin, en fonction du niveau de chiffrement qu'ils offrent[52].

1 Pour ne pas compliquer la lecture, nous utilisons le masculin de manière générique pour désigner également le féminin.

2 Cette analyse se fonde sur l'état de la technologie au moment de la rédaction du présent article, qui peut rapidement évoluer.

3 On peut par exemple présumer que des informations fiscales pourront intéresser des gouvernements étrangers.

4 Nous ne traiterons pas dans cet article du risque de la communication en tant que vecteur d'attaque (p.ex. pour insérer des logiciels malveillants).

5 *Infra,* II.3.

6 *Infra,* II.4.

7 Aucune forme particulière n'est requise pour l'accord du client: cf. Chappuis/Gurtner, La profession d'avocat, 2021, Nos 909–910, p. 238.

8 Il reste néanmoins utile de l'avertir de manière générale par une clause dans la convention de mandat. Pour un exemple, voir: *Indications et recommandations de la FSA pour la sous-traitance informatique et l'utilisation de services cloud,* juin 2019, p. 17.

9 Chappuis/Gurtner, *op. cit.,* Nos 942 et 946, p. 246.

10 Benhamou/Erard/Kraus, L'avocat a-t-il aussi le droit d'être dans les nuages?, Revue de l'avocat 3/2019; Schwarzenegger/Thouvenin/Stiller/George, Utilisation de services cloud par les avocats, Revue de l'Avocat 1/2019;Chappuis/Alberini, Secret Professionnel de l'Avocat et Solutions Cloud, Revue de l'Avocat 8/2017.

11 La divulgation du secret professionnel nécessite en effet qu'un tiers (qui n'est pas auxiliaire) en prenne connaissance; voir Schwarzenegger/Thouvenin/Stiller/George, *op. cit.,* p. 36 et les références citées.

12 Chappuis/Alberini, *op. cit.,* p. 340; Schwarzenegger/Thouvenin/Stiller/George, *op. cit.,* p. 37.

13 Schwarzenegger/Thouvenin/Stiller/George, *op. cit.,* p. 36.

14 ATF 145 II 229, c.7.2; Chappuis/Alberini, *op. cit.,* p. 340.

15 RS 235.1.

16 Loi fédérale du 25. 9. 2020 sur la protection des données (https://www.fedlex.admin.ch/eli/fga/2020/1998/fr) (tous les liens de cet article consultés la dernière fois le 28.3.2022).

17 Ce qui est vrai même pour des données sensibles: voir Jotterand/Erard, Recherche sur l'être humain et données personnelles, Jusletter 30.8.2021, N 88 (p. 31).

18 *Supra,* II.3.

19 Schwarzenegger/Thouvenin/Stiller/George, *op. cit.,* p. 39.

20 Ces éléments sont décrits dans le guide du PFPDT pour vérifier l'admissibilité des transferts directs ou indirects de données vers l'étranger, du 28.6.2021.

21 https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087

22 Sur l'application de cette obligation aux études d'avocats, voir Straub/Bhend, Informatique et protection des données dans la convention de mandat, Revue de l'avocat 10/2021, pp. 414–415.

23 Pour la Suisse, cf. les art. 19 al. 1 let. b et 21 al. 2 LSCPT, qui imposent une conservation des données secondaires de télécommunication, ainsi que les caractéristiques techniques des envois postaux durant six mois.

24 Même si d'autres personnes peuvent avoir accès à la boîte mail.

25 Chappuis/Gurtner, *op. cit.,* Nos 1222.1223, p. 321.

26 *Les fax menacent la sécurité des entreprises,* in Le Temps du 20.8.2018 (https://www.letemps.ch/economie/fax-menacent-securite-entreprises); Chappuis/Gurtner, *op. cit.,* No 1224, p. 321.

27 Adrian Fufener, «Clic informatique» – devrions-nous sécuriser les e-mails échangés avec nos clients? Revue de l'Avocat 9/2011, p. 380.

28 Sébastien Fanti, Courrier électronique et responsabilité de l'avocat, Revue de l'Avocat 11–2011, p. 493.

29 L'on pense ici aux programmes de la NSA. Toutefois, le Service de renseignement de la Confédération (SRC) est également autorisé à *«enregistrer les signaux transmis par réseau filaire qui traversent la frontière suisse»* sur la base de mots-clés (art. 39 al. 1. de la loi fédérale sur le renseignement; RS 121).

30 Il faut savoir que les e-mails transitent par différents serveurs entre leur envoi et leur réception et peuvent être stockés dans le nuage (cloud).

31 Selon les informations publiées par Google, entre 80 et 90% des e-mails qui sont expédiés ou reçus par cette société sont désormais chiffrés selon le protocole TLS (ce qui signifie que dans le reste des cas, l'autre fournisseur de messagerie concerné ne prend pas en charge le protocole TLS). Voir https://transparencyreport.google.com/safer-email/overview

32 Selon le protocole *«opportunistic TLS»,* le fournisseur va d'abord essayer de chiffrer la connexion avec la version la plus sécurisée de TLS, puis va essayer, en cas d'échec, des niveaux de sécurité inférieurs jusqu'à ce qu'il en trouve un en commun avec le fournisseur de destination (potentiellement aucun chiffrement TLS). Pour parer à cela, il est en général possible de configurer sa messagerie pour

«forcer» TLS, ce qui implique toutefois que l'e-mail ne sera pas envoyé si le fournisseur du destinataire ne supporte pas TLS (voir https://docs.microsoft.com/en-us/microsoft-365/compliance/exchange-online-uses-tls-to-secure-email-connections?view=o365-worldwide).

33 C'est également l'opinion de l'American Bar Association. Voir sa *Formal Opinion 477R** (Securing Communication of Protected Client Information), dans sa version du 22.05.17. Contra: Déborah Lechtman, L'obligation de «privacy by design» en Suisse et son implémentation dans les Études d'avocats, Revue de l'Avocat 10/2020, p. 406, selon qui un avocat ne devrait pas communiquer avec un client utilisant une messagerie Gmail, sans toutefois donner plus de précision sur la nature du risque fondant cette évaluation.

34 L'autre protocole couramment utilisé est PGP (pour *Pretty Good Privacy*). À la différence de S/MIME, PGP fonctionne au moyen d'une paire de clés pour chiffrer et déchiffrer un e-mail, et non de certificats numériques.

35 Tous deux doivent avoir un certificat personnel valide acquis auprès d'une autorité de certification. L'expéditeur doit au demeurant disposer de la clé publique du destinataire, ce qui nécessite en général d'avoir au préalable reçu un e-mail signé de ce dernier (*supra,* III.3.B).

36 Si l'on se donne la peine de chiffrer de bout en bout un e-mail, mieux vaut donc faire attention à ce que l'on indique dans son objet.

37 La seule solution à ce problème est d'effectuer une recherche de logiciels malveillants sur les postes des utilisateurs finaux après le déchiffrement. Il en va de même de la détection des *spams* et tentatives de *phishing*.

38 Il existe d'autres mesures pour parer à ce risque, que nous ne détaillerons pas ici.

39 ProtonMail offre un chiffrement selon la norme PGP dont la mise en place *«n'est pas simple et n'est pas à la portée de tous»*selon les propres déclarations de la société: (https://protonmail.com/support/knowledge-base/how-to-use-pgp/).

40 *Supra,* II.3. et II.4.

41 Accessible sous https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_messenger_videokonferenzsysteme.pdf

42 https://noyb.eu/sites/default/files/2020-04/noyb_-_report_on_privacy_policies_of_video_conferencing_tools_2020-04-02_0.pdf

43 Voir le DPIA réalisé à la demande du gouvernement hollandais, section 9, état au 25.2.2022 (https://www.surf.nl/zoom-past-privacyvoorwaarden-aan-na-intensief-overleg-met-surf). Zoom a également publié, suite à ce DPIA, une Privacy Data Sheet (https://explore.zoom.us/media/privacy-data-sheet-feb.pdf) et apporté des améliorations à son accord sur la protection des données (https://explore.zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf). Zoom publie également des informations sur les requêtes qu'elle reçoit d'autorité (https://explore.zoom.us/docs/en-us/trust/transparency.html).

44 Hürlimann/Steiger, Auf dem Weg zur digitalen Anwaltskanzlei trotz Berufsgeheimnis und Datenschutz. Revue de l'Avocat 5/2021, p. 204; David Rosenthal, Microsoft Cloud für Schweizer Anwälte, Revue de l'Avocat 10/2021.

45 https://techcommunity.microsoft.com/t5/microsoft-teams-blog/end-to-end-encryption-for-one-to-one-microsoft-teams-calls-now/ba-p/3037697

46 Notamment des mesures de chiffrement fort (chiffrement à double clé) ou le système «Customer Lockbox». Voir le DPIA réalisé à la demande du gouvernement hollandais, état au 16.2.2022 (https://www.rijksoverheid.nl/documenten/publicaties/2022/02/21/public-dpia-teams-onedrive-sharepoint-and-azure-ad).

47 EDPS Decision authorising temporarily use of CJEU-Cisco ad hoc clauses for transfers (Cisco Webex), 31.8.2021 (https://edps.europa.eu/data-protection/our-work/publications/authorisation-decisions-transfers/edps-decision-authorising-0_en).

48 Selon les informations fournies par Jitsi: https://jitsi.org/security/.

49 *Voici comment choisir entre Signal, Threema et Telegram,* in Le Temps (17.01.21) (https://www.letemps.ch/economie/voici-choisir-entre-signal-threema-telegram).

50 Sous réserve des principes généraux développés dans cet article, en particulier le respect de la volonté du client (*supra,* II.2.).

51 P.ex. une haute probabilité que des tiers non autorisés cherchent à accéder à la communication et puissent effectivement le faire.

52 Ces recommandations sont inspirées de celles de l'*American Bar Association* dans sa *Formal Opinion 477R** (Securing Communication of Protected Client Information), version du 22.05.17 (https://www.americanbar.org/news/abanews/publications/youraba/2017/june-2017/aba-formal-opinion-477r--securing-communication-of-protected-cli/).