Conseil des barreaux européens
La voix des avocats européens
Rue Joseph II, 40/8 - B-1000 Bruxelles
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

Lignes directrices du CCBE sur l'utilisation des outils de travail à distance par les avocats et les procédures judiciaires à distance

27/11/2020

Le Conseil des barreaux européens (CCBE) représente les barreaux de 32 pays membres et de 13 autres pays associés et observateurs, soit plus d'un million d'avocats européens.

Dans ce document, le CCBE souhaite fournir aux avocats quelques conseils sur l'utilisation des outils de travail à distance et sur la conduite des procédures judiciaires à distance.

I. Introduction

On dit souvent que les événements perturbateurs peuvent parfois mener à des changements radicaux dans la manière de faire les choses, mais qu'ils accélèrent plus souvent des tendances qui se développent lentement depuis des années.

Cela est particulièrement évident en ce qui concerne l'effet que la Covid-19 a eu sur la manière dont les avocats exercent leurs fonctions et interagissent avec les tribunaux. Par exemple, depuis quelques années, un certain nombre de juridictions acceptent de plus en plus d'audiences dont au moins un des participants (par exemple, les personnes poursuivies dans les audiences de procédure ou certains témoins à un procès) assiste à distance. Toutefois, jusqu'aux défis posés par la pandémie de Covid-19, seules quelques premières timides étapes avaient été mises en œuvre en vue de la tenue d'audiences entièrement accessibles à distance. Les restrictions de circulation imposées par les réglementations liées à la crise de Covid-19 dans la plupart des pays européens ont accéléré ces mesures auparavant lentes et timides.

À bien des égards, les systèmes juridiques se sont retrouvés en terrain inconnu et ont utilisé des outils nouveaux et peu familiers. Il ne fait aucun doute que de nombreux avocats connaissaient déjà d'anciens outils commerciaux tels que les conférences téléphoniques et qu'ils avaient au moins une connaissance limitée des applications des réseaux sociaux telles que Facebook Messenger et Skype, mais les conférences téléphoniques présentent des limites évidentes, et ce qui peut convenir à l'échange de civilités et de photos d'animaux n'est pas nécessairement adapté à l'administration de la justice et à la conduite de discussions qui relèvent du secret professionnel ou du *legal professional privilege*.

L'utilisation des outils de téléconférence présente deux aspects interdépendants :

- les consultations et réunions des avocats avec leurs clients et d'autres personnes par des moyens à distance ;
- la participation aux audiences à distance.

Les questions relatives à chaque aspect présentent un certain degré de similitude, mais chacune d'entre elles soulève également des problèmes particuliers.

II. L'utilisation d'outils de travail à distance par les avocats

Il existe un besoin évident de réunions à distance, que ce soit avec les clients, l'interrogation de témoins potentiels, les réunions de gestion interne, les négociations avec d'autres parties : tout ce qui se réalisait normalement en face-à-face dans un cabinet d'avocats doit désormais se faire en ligne. Au début de la pandémie, un certain nombre d'outils étaient déjà disponibles, mais le défi pour les fournisseurs était de faire face à l'augmentation de leur utilisation, et pour l'utilisateur de faire usage d'outils qui avaient été développés pour un environnement et de les développer pour un autre environnement plus difficile tel que celui de la pratique juridique avec son exigence absolue de confidentialité.

Dans ce contexte, les aspects suivants se détachent :

(a) *Droits fondamentaux : Les* questions relatives aux droits fondamentaux se poseront clairement dans tous les cas où le secret professionnel/*legal professional privilege* entre en jeu mais peuvent l'être de manière légèrement différente. Toutes les communications seront protégées en vertu de l'article 8 de la CEDH, qu'elles soient liées à un litige potentiel ou en cours, à des négociations commerciales, des conseils en matière de droit du travail, des transactions immobilières ou tout autre domaine parmi une myriade d'autres de nature non contentieuse dans lesquels des conseils juridiques peuvent être impliqués, tandis que les communications relatives aux procédures pénales ou aux litiges commerciaux et autres seront également protégées en vertu de l'article 6 de la CEDH. Il convient de noter que les droits de l'article 8 de la CEDH sont conditionnels (bien que les communications entre avocats et clients bénéficient d'un niveau de protection plus élevé), tandis que les droits de l'article 6 de la CEDH sont absolus.

(b) *Secret professionnel/legal professional privilege :* Cette règle s'applique de façon claire, que le client soit une personne physique ou morale.

(c) *Respect du RGPD* : Cela concerne les personnes concernées qui sont des personnes physiques, il est donc évident qu'elles auront affaire à des clients qui sont des personnes physiques. L'implication du RGPD lorsque le client est une personne morale peut ne pas sembler si évident mais il est probable qu'il faille en pratique traiter des données à caractère personnel concernant des personnes physiques, qu'il s'agisse d'employés, de clients, de personnes avec lesquelles des négociations sont menées, etc. étant donné que des personnes physiques se trouvent derrière chaque entité juridique.

Il s'agit de sujets de préoccupation qui doivent être soigneusement pris en compte lors de l'examen des conditions générales des différents fournisseurs de plateformes. Une telle analyse est souvent loin d'être simple, notamment en raison du fait que les conditions générales applicables ne sont pas nécessairement regroupées en un tout cohérent au sein d'une seule et même rubrique sur le site Internet concerné. Ce dont un utilisateur a besoin de savoir pour assurer le respect du RGPD et des obligations déontologiques est souvent dispersé entre un certain nombre de documents : conditions générales, politiques de confidentialité, annexes, etc., chacun d'entre eux pouvant se trouver dans des rubriques totalement différentes d'un site Internet sans pour autant faire nécessairement l'objet d'un lien hypertexte ou d'un index croisé.

Afin d'essayer de comprendre les questions pratiques qui se posent en matière de pratique juridique, le CCBE a préparé un certain nombre de documents de recherche individuels examinant les conditions générales d'un certain nombre de plateformes fréquemment utilisées afin de les comparer[1]. Cet exercice a permis de dégager certaines questions communes, à savoir :

[1] Ces documents peuvent être consultés à l'adresse [https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20201127_Annex_Analyses-of-videoconferencing-tools.pdf] et peuvent constituer un point de départ pour une analyse plus approfondie. Toutefois, étant donné la rapidité avec laquelle le domaine évolue, il convient de souligner que les

1. Dans quelle mesure les conditions générales applicables sont-elles accessibles et transparentes ?
2. Qui est responsable du traitement des données ?
3. Où sont conservées les données ?
4. Dans quelle mesure les fournisseurs de plateformes vendent-ils ou partagent-ils des données personnelles ?
5. À quelle surveillance les données détenues par les fournisseurs de plateformes dans le nuage pourraient-elles être exposées ?
6. Quel est le niveau de sécurité technique de la plateforme ?

1. Accessibilité et transparence

Il a été question plus haut de la difficulté que l'on rencontre fréquemment lorsqu'on essaie de déterminer les conditions générales et les politiques de protection de la vie privée qui sont applicables à un moment donné. Cette difficulté est aggravée par le fait que les fournisseurs de plateformes modifient fréquemment les conditions et les politiques de protection de la vie privée, parfois en publiant de nouvelles éditions, parfois en apportant des modifications non annoncées aux conditions existantes qui, souvent, ne sont même pas mises en évidence, de sorte que le seul moyen de détecter un changement est de comparer soigneusement l'ancien texte et le nouveau.

Il ne s'ensuit pas nécessairement que la difficulté d'accès soit liée à un désir de cacher des termes malheureux par exemple, la manière dont toutes les conditions pertinentes de Cisco Webex sont présentées est d'une telle complexité byzantine que même le Centre européen pour la défense des droits numériques, dans son rapport sur les politiques de confidentialité des services de vidéoconférence[2], a analysé les conditions de Cisco comme n'étant pas entièrement conformes au RGPD, bien que les recherches du CCBE aient révélé par la suite que les auteurs du rapport n'avaient pas trouvé un certain nombre de documents contractuels pertinents qui se trouvaient (sans hyperlien) ailleurs sur le site web. En examinant l'ensemble des conditions contractuelles, Cisco Webex respectait davantage le RGPD que ce que le rapport indiquait.

Ce manque de transparence des conditions générales a fait l'objet de commentaires de la part du Contrôleur européen de la protection des données[3].

Tout au long des différents documents de recherche du CCBE, il a été noté que le manque de clarté n'est pas nécessairement intentionnel et qu'il est parfois désavantageux non seulement pour le client mais aussi pour le fournisseur de la plateforme. Quoi qu'il en soit, il est vrai que les conditions générales des plateformes contiennent souvent des dispositions complexes et des exceptions. En outre, nombre d'entre elles doivent être complétées par d'autres documents (normalement également disponibles sur la page web) tels que des déclarations et des suppléments de confidentialité ou des accords par défaut sur le traitement des données.

2. Qui est le responsable du traitement des données ?

documents peuvent ne pas refléter les changements introduits par les prestataires après la réalisation de la recherche. Il en va de même pour les références à des prestataires spécifiques dans le texte.

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

[3] Le Contrôleur européen de la protection des données (CEPD) a également examiné cette question dans son document public sur les résultats de l'enquête d'initiative sur l'utilisation par les institutions européennes des produits et services Microsoft (2 juillet 2020), voir la partie 6

Les fournisseurs de plateformes sont en quelque sorte dans une courbe d'apprentissage en raison de l'utilisation accrue de leurs plateformes par un nombre croissant d'utilisateurs dans des secteurs de plus en plus variés. Certains fournisseurs, notamment certains de ceux qui sont basés aux États-Unis, ont pris conscience qu'ils devaient respecter les obligations du RGPD et qu'ils devaient maîtriser une nouvelle terminologie juridique.

De ce fait, ils affirment parfois des choses qui ne sont manifestement pas le cas. Par exemple, jusqu'à récemment, Zoom affirmait ne jamais pouvoir être responsable du traitement des données à caractère personnel qu'elle traitait, et Microsoft, bien qu'adoptant une approche plus nuancée, reste critiquable de n'avoir pas pleinement analysé les situations dans lesquelles il pourrait effectivement être responsable du traitement des données. En particulier, l'enquête du CEPD sur l'utilisation des produits et services de Microsoft par les institutions européennes évoquée ci-dessus a précisé que Microsoft (ainsi que d'autres fournisseurs) peut agir en tant que responsable du traitement des données d'une manière qui n'est pas toujours transparente, comme par exemple : les droits des fournisseurs de services de modifier unilatéralement les conditions de protection des données, la portée limitée des obligations en matière de protection des données dans les conditions générales et l'absence de finalités spécifiquement définies pour le traitement réalisé dans le cadre de ces conditions.

Si certaines plateformes se considèrent responsables du traitement des données (par exemple Kinly et Messenger Video), les conditions générales d'autres plateformes définissent le client comme responsable du traitement des données, la plateforme n'en étant que sous-traitant. Même dans ce dernier cas, tel que cela a pu être observé, les dispositions des conditions générales, prises dans leur ensemble, peuvent fonctionner de manière à conférer au fournisseur de plateforme des pouvoirs si étendus qu'il agit en réalité également comme responsable du traitement des données malgré les déclarations contraires dans les conditions générales[4]. C'est le cas par exemple de Zoom (jusqu'à une récente modification de ses conditions générales), de Microsoft Teams et de Cisco.

3. Où les données sont-elles conservées ?

Les conditions générales de nombreuses plateformes ne garantissent pas que les données soient conservées dans un pays en particulier, ni même au sein de l'UE. Cette situation pose de toute évidence un problème de conformité au RGPD.

Dans le cas de plateformes telles que Messenger Video, Skype, Skype for Business, BlueJeans et Cisco, il est clair que les données collectées dans l'Union européenne peuvent être transférées et conservées en dehors de l'UE (principalement mais pas uniquement aux États-Unis). Dans certains autres cas, il n'est pas facile d'identifier l'État dans lequel les données seront conservées en raison de l'existence de plusieurs centres de données, ce qui semble par exemple être le cas de Kinly et StarLeaf. Un autre exemple est celui de Microsoft Teams, dont les modalités, selon le pays où se trouve le responsable du traitement des données (c'est-à-dire le client) et selon le type de données, en font varier le lieu de conservation. Il est important de noter qu'au moins une partie des données que les responsables du traitement des données de nombreux pays de l'UE contrôlent est conservée hors de l'UE[5]. Cela pourrait suggérer que la diligence raisonnable devrait inclure le fait de chercher, dans la mesure du possible, à utiliser des plateformes dont les serveurs sont hébergés dans l'UE et que, si cela est impossible, de chercher à se conformer aux recommandations et aux décisions de la Commission européenne, de

[4] Le Contrôleur européen de la protection des données (CEPD) a également examiné cette question dans son document public sur les résultats de l'enquête d'initiative sur l'utilisation par les institutions européennes des produits et services Microsoft (2 juillet 2020), voir la partie 2

[5] Le Contrôleur européen de la protection des données (CEPD) a également examiné cette question dans son document public sur les résultats de l'enquête d'initiative sur l'utilisation par les institutions européennes des produits et services Microsoft (2 juillet 2020), voir la partie 4

l'EDPB et des autorités nationales compétentes en matière de protection des données en ce qui concerne les transferts internationaux de données.

Le problème est aggravé par le fait que de nombreux fournisseurs basés aux États-Unis s'appuyaient sur l'autocertification dans le cadre du bouclier de protection des données UE-États-Unis pour régulariser ces transferts de données, mais la décision de la Cour européenne de justice dans l'affaire *Schrems II*[6], annulant le bouclier de protection, a empêché l'utilisation de ce mécanisme. Bien que l'arrêt confirme la validité des clauses contractuelles types, une vigilance constante s'impose. La Cour européenne de justice a indiqué que la nécessité de garanties supplémentaires doit être vérifiée au cas par cas, c'est pourquoi le débat sur l'efficacité de telles clauses se poursuit.

4. Dans quelle mesure les fournisseurs de plateformes vendent-ils ou partagent-ils des données personnelles ?

Les conditions générales de la plupart des fournisseurs de plateformes indiquent en général que les données ne seront ni vendues ni partagées, sauf dans la mesure où les conditions générales elles-mêmes le permettent.

Parfois, ces déclarations ne doivent pas être prises au pied de la lettre étant donné que la partie des conditions générales dans laquelle figurent les définitions peut donner des sens spécifiques à des termes tels que « vendre ». Par exemple, les conditions d'un fournisseur indiquent que le transfert de données à une autre personne pour un paiement ne compte pas comme « vente » si les conditions du bénéficiaire du transfert sont similaires à celles du fournisseur.

En outre, dans le cadre des conditions générales, il existe généralement des exceptions en vertu desquelles les fournisseurs peuvent bien partager les données des clients avec certains tiers sous certaines conditions. Les conséquences de ces exceptions ne sont souvent pas claires. Par exemple, la plupart des fournisseurs de plateformes sont autorisés à partager, si nécessaire, des données avec des tiers tels que des partenaires commerciaux, des auditeurs, des conseillers juridiques, des filiales et des sociétés affiliées. Ils peuvent également partager des données pour d'autres raisons, notamment pour se conformer à des obligations juridiques ou dans le cadre de transactions d'entreprise telles que des fusions ou des ventes d'actifs. Dans certains cas, le manque de transparence des conditions générales et de prévisibilité de leur effet est particulièrement problématique, des exceptions larges et vagues permettant le partage de données pour des raisons telles que l'application de la politique et des accords du fournisseur de la plateforme, la mise en œuvre de ses opérations commerciales ou la protection de son droit de propriété.

5. À quelle surveillance les données détenues par les fournisseurs de plateformes dans le nuage pourraient-elles être exposées ?

Une préoccupation particulière à cet égard réside dans le danger que représentent les nombreux fournisseurs de plateformes de premier plan qui sont basés ou implantés aux États-Unis, où ils sont soumis à la juridiction de grande portée de la loi sur les nuages « Cloud Act ». Le Cloud Act permet aux tribunaux et aux autorités des États-Unis de demander des données à caractère personnel aux entreprises américaines qui les conservent sur des serveurs en nuage au sein de l'Union européenne. Le Comité européen de la protection des données (EDPB) et le Contrôleur européen de la protection des données (CEPD) ont abordé la question de la justification des transferts de données dans le cadre du Cloud Act dans une réponse conjointe à la commission LIBE. Dans cette réponse, ils estiment qu'en cas de demande reposant sur le Cloud Act sans accord international correspondant à l'article 48 RGPD,

[6] *Arrêt du 16 juillet 2020, affaire Schrems II*

un transfert de données ne peut être justifié que s'il est nécessaire pour protéger les intérêts vitaux des personnes concernées[7].

6. Quel est le niveau de sécurité technique de la plateforme ?

La sécurité technique des plateformes ne semble pas être un problème majeur, mais il existe néanmoins quelques failles.

Certaines de ces failles sont liées aux paramètres par défaut de l'utilisateur et peuvent facilement être corrigées si l'utilisateur est conscient du risque et prend des mesures pour modifier les paramètres utilisateur. Par exemple, il est notoire qu'au début du confinement, les paramètres utilisateur par défaut de Zoom ont été réglés à des niveaux de sécurité minimums, permettant un accès très facile aux participants non autorisés, et donnant un nouveau mot à la langue anglaise : *Zoom-bombing*. Les utilisateurs pouvaient ajuster les paramètres pour obtenir un meilleur niveau de sécurité, mais il est remarquable de constater que nombre d'entre eux n'ont pas pris les mesures nécessaires. Cependant, étant sensible aux pressions du marché, Zoom a réagi en modifiant ses paramètres par défaut pour offrir des niveaux de sécurité plus élevés, et ce problème particulier a maintenant largement disparu.

Il existe cependant d'autres failles de sécurité qui sont inhérentes aux plateformes et qui ne sont pas si faciles à résoudre. Cela est d'autant plus vrai en ce qui concerne la nature et l'étendue du chiffrement fourni.

Certaines plateformes, mais pas toutes, offrent un chiffrement de bout en bout. Microsoft, par exemple, propose un chiffrement de bout en bout, tandis que d'autres plateformes, telles que Cisco, proposent un chiffrement standard par défaut, le chiffrement de bout en bout n'étant qu'une option supplémentaire. Il a été rapporté que d'autres plateformes comme Zoom offraient au début du confinement un « chiffrement » qui n'était ni de bout en bout ni conforme aux normes internationales en matière de chiffrement, bien que Zoom ait résolu le problème depuis.

7. Y a-t-il des obstacles à la disponibilité des recours ?

Les conditions générales contiennent généralement des clauses d'élection de for et des clauses attributives de juridiction. Il convient de garder à l'esprit que ces clauses (en particulier la dernière) peuvent constituer des obstacles pratiques à l'obtention de recours. Cela est d'autant plus problématique que de nombreux fournisseurs disposent de clauses conférant une compétence exclusive à un État particulier ou à la juridiction fédérale des États-Unis (voire parfois à un tribunal déterminé dans une ville déterminée) bien que certains, notamment Cisco, prévoient au moins la compétence d'une juridiction européenne.

<u>Conclusion concernant la téléconférence</u>

Comme le révèle ce qui précède, il est toujours nécessaire que les avocats lisent, comprennent et revoient régulièrement les conditions générales des plateformes qu'ils utilisent afin de s'assurer qu'ils respectent correctement leurs obligations en matière de protection des données et de déontologie.

Les diverses plateformes offrent des normes différentes en matière de fiabilité, de robustesse, d'expérience utilisateur et d'autres aspects. Il peut y avoir une tendance naturelle à choisir celle qui offre, subjectivement, la meilleure expérience et les fonctionnalités les plus utiles. C'est en grande partie une question de goût mais, en fin de compte, le choix d'un outil adéquat dépend non seulement de ces facteurs, mais aussi d'un examen attentif des grands inconnus : respect du RGPD, protection de

[7] ANNEXE. Première évaluation juridique des effets du US CLOUD Act sur le cadre juridique de l'UE pour la protection des données à caractère personnel et les négociations d'un accord UE-États-Unis sur l'accès transfrontalier aux preuves : https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf

la confidentialité, robustesse des conditions générales du point de vue de l'utilisateur. En outre, comme le révèle ce qui précède, il s'agit d'un exercice de révision qui ne peut être effectué une seule fois mais doit être réalisé de manière constante.

III. Procédures judiciaires à distance

Divers tribunaux de différentes juridictions mènent des procédures à distance en utilisant différentes plateformes. Bien que les mêmes problèmes que ceux évoqués ci-dessus se posent toujours, ils sont probablement moins préoccupants en pratique pour les avocats étant donné que ce sont les tribunaux qui sont susceptibles d'être responsables du traitement des données plutôt que les avocats. En tout état de cause, les procédures judiciaires sont généralement publiques et, dans certaines juridictions, les pièces mentionnées au tribunal deviennent publiques. Dans certaines juridictions, il se peut également que les divulguer au juge et à l'autre partie signifie qu'elles ne relèveront plus du secret professionnel/*legal professional privilege*.

Cela ne signifie pas pour autant que les barreaux et les avocats peuvent ignorer les questions de protection de la vie privée et des données. Un exemple concret : en Angleterre et au pays de Galles où, à un stade précoce de la pandémie, les services judiciaires ont proposé que les procédures devant le juge aux affaires familiales en Angleterre et au Pays de Galles se fassent sur Zoom. Cette proposition était d'autant plus préoccupante que les données résultant de ces procédures sont souvent des catégories particulières de données à caractère personnel et que ces procédures se dérouleront normalement à huis clos. Il était donc nécessaire de signaler à l'administration judiciaire ces préoccupations particulières ainsi que les préoccupations génériques qui avaient été exprimées au sujet de la plateforme Zoom dans l'état où elle se trouvait à l'époque.

La question de la garantie d'un procès équitable conformément à l'article 6 de la CEDH est davantage susceptible de susciter des inquiétudes au jour le jour. Il convient de noter en particulier l'obligation de disposer de canaux privés parallèles sécurisés accessibles aux clients respectifs et à leur équipe juridique[8].

La plupart des tribunaux semblent ne pas offrir cette possibilité, mais que les équipes juridiques concernées prennent leurs propres dispositions *ad hoc* (plateformes séparées, courrier électronique, groupes de discussion sur diverses plateformes, etc.). La question se pose de savoir si cela est juridiquement adéquat pour garantir un procès équitable, en particulier lorsque les parties adverses ont des niveaux d'expertise technique différents, et que des problèmes pratiques se posent quant à la meilleure façon d'utiliser ces canaux parallèles.

De manière plus significative, les mêmes questions se posent concernant les réunions à distance tel qu'indiqué plus haut lorsque les avocats fournissent leurs propres canaux. Par exemple, si un avocat mettait en place un canal parallèle en utilisant, par exemple, un groupe de discussion sur Facebook Messenger, la discussion (qui relèverait du secret professionnel/*legal professional privilege*) serait conservée par Facebook sur ses serveurs et soumise à une surveillance en vertu du Cloud Act. Le support utilisé pourrait peut-être être WhatsApp, qui est certainement plus sûr d'un point de vue technique. Cependant, le problème reste que le support utilisé pour ce canal parallèle pourrait ne pas être celui utilisé par l'avocat pour d'autres affaires à distance, ce qui ne dispense pas l'avocat d'exercer, par rapport à ce canal, le même type de diligence raisonnable qui doit être exercée pour déterminer quelle installation de téléconférence utiliser.

Il existe d'autres questions qui ne sont pas de nature purement informatique ou liées à la surveillance et qui sont inhérentes aux procédures à distance, par exemple, en ce qui concerne l'égalité des armes : désavantage pour les parties n'ayant pas accès à l'informatique, effet des faibles débits Internet, difficulté pour un juge d'évaluer efficacement la crédibilité d'un témoin sans le voir en chair et en os,

---

[8] Sakhnovskiy c. Russie (Requête n° 21272/03) et Marcello Viola c. Italie (Requête n° 45106/04).

problèmes de sécurité des connexions à distance (comment savoir si, métaphoriquement ou littéralement, l'homme qui tient la caméra devant le témoin ne tient pas également une arme ?). Il est certain que ces arguments ne peuvent pas être entièrement exclus dans une procédure réelle : il est également possible de faire valoir que les parties n'ayant pas accès aux technologies de l'information n'ont pas non plus les moyens de se payer une assistance juridique et qu'un témoin peut être influencé d'autres manières avant une audience, par exemple par des menaces. Quoi qu'il en soit, il est nécessaire de les prendre en considération.

Ces questions et d'autres ont été discutées dans un document du CCBE sur l'utilisation de la vidéoconférence dans les affaires pénales et civiles reposant sur la position du CCBE sur les propositions de modification des règlements sur la signification et la notification des actes et l'obtention des preuves en matière civile et commerciale (19/10/2018). Les remarques générales suivantes formulées dans ce document, qui sont pertinentes pour les procédures civiles mais d'autant plus dans les procédures pénales et civiles, méritent également d'être soulignées ici :

- Avant d'établir un programme de vidéoconférence, les tribunaux ou autorités judiciaires devraient mettre en œuvre leur système de vidéoconférence par le biais d'un programme pilote qu'ils peuvent évaluer et modifier. Les tribunaux devraient mettre en place un système dans lequel, à la suite d'une vidéoconférence, ils reçoivent des commentaires de toutes les parties prenantes (y compris les avocats) sur l'organisation de la vidéoconférence afin d'améliorer le système. De plus, les tribunaux devraient offrir une formation structurée aux juges et à toute personne qui exploitera le matériel de vidéoconférence pendant l'audience, ainsi qu'au personnel informatique. Ils devraient également partager entre eux les bonnes pratiques en matière de vidéoconférence afin de réduire les frais et être plus efficaces.

- Des plans d'urgence doivent être mis en place afin de résoudre efficacement les problèmes tels que les pertes de connexion ou une mauvaise connexion en cours de vidéoconférence.

- Dans les affaires transfrontalières, en particulier lorsque les parties n'ont pas la même langue maternelle et sont soumises à des influences culturelles différentes, il se peut que le juge ne puisse pas examiner si facilement par vidéoconférence les nuances dans les comparutions et les réponses des parties. En outre, le juge pourrait avoir tendance à poser moins de questions et à être moins enclin à interrompre une observation orale en vidéoconférence, ce qui pourrait ne pas être bénéfique pour les parties[9]. Par conséquent, il est important d'élaborer des normes minimales obligatoires pour les aménagements techniques à mettre en place pour l'utilisation de la vidéoconférence de manière à garantir autant que possible une véritable audience avec une communication et une interaction complète de toutes les parties à la procédure avec le témoin ou la personne examinée. Les services de vidéoconférence destinés aux consommateurs, tels que Skype ou FaceTime, ne sont pas adéquats.

- Dans certaines juridictions, l'utilisation de la vidéoconférence peut être soumise à l'approbation des parties. Les questions pertinentes sont donc : Est-il nécessaire de demander le consentement des parties pour participer à une vidéoconférence ? Dans quelles conditions les parties peuvent-elles refuser une vidéoconférence ? Un avocat doit-il être présent ou consulté si les parties y consentent ou refusent ?

- La question extrêmement importante de la garantie du respect du secret professionnel/*legal professional privilege* lors de l'utilisation de différents outils en ligne pour des procédures à distance a déjà été abordée ci-dessus. Comme il a également été noté, lors d'une séance par vidéoconférence, l'avocat doit pouvoir s'entretenir confidentiellement avec son client (aussi bien si l'avocat et le client sont assis l'un à côté de l'autre que s'ils se trouvent à distance l'un de l'autre). Les questions qui se posent sont donc les suivantes : la confidentialité de la

[9] Voir par exemple *Report of a Survey of Videoconferencing in the Court of Appeals, M. Dunn and R. Norwick, Federal Judicial Center,* 2006, disponible sur https://www.fjc.gov/content/report-survey-videoconferencing-courts-appeals-0.

communication avocat-client est-elle garantie dans toutes les juridictions participant à la vidéoconférence ? Si ce n'est pas le cas, les intérêts des parties pourraient être compromis. La vidéoconférence peut-elle être enregistrée ? En cas de violation de la confidentialité impliquant une vidéoconférence, qui en assume la responsabilité professionnelle ? Quelles sont les exigences techniques à respecter afin de garantir que la vidéoconférence est protégée contre un accès non autorisé (piratage) ?

- Le tribunal ou l'autorité judiciaire doit notifier aux parties, y compris à leurs avocats, les données, l'heure, le lieu et les conditions de participation à la vidéoconférence. Un préavis suffisant doit être donné. Dans ce contexte, quel doit être le délai pour que le préavis soit considéré comme suffisant ?

- Des dispositions doivent être prises pour permettre à l'avocat de participer à la vidéoconférence. L'avocat doit être en mesure de s'asseoir avec son client. Si cela n'est pas possible, des dispositions doivent être prises pour permettre à l'avocat de participer à la vidéoconférence à partir d'un autre lieu.

- Lorsque les règles locales exigent qu'un avocat participant fournisse des preuves de son identité et de son droit à comparaître, il doit être habilité à le faire, à distance si nécessaire.

- Le tribunal ou l'autorité judiciaire compétente doit fournir des instructions à l'avocat quant à la procédure à suivre pour présenter des pièces ou d'autres éléments lors de la vidéoconférence. Des dispositions doivent être prises pour s'assurer que tous les participants à la vidéoconférence peuvent voir les éléments présentés pendant la vidéoconférence.

- Lorsque des actes doivent être présentés à un témoin, le soin devrait en être confié à une personne indépendante présente (greffier ou membre du personnel semblable) pouvant s'assurer (par exemple du point de vue du plaignant) qu'il regarde la page correcte et (du point de vue du défendeur) qu'il ne voit pas d'autre acte, plus particulièrement ceux n'ayant pas été divulgués au défendeur ou à d'autres parties.

Ces préoccupations concernent tant les procédures pénales que civiles. Toutefois, la réponse à la question de savoir si, dans un cas précis, une procédure à distance peut être considérée comme un moyen approprié de mener une procédure diffère certainement selon la nature de l'affaire (c'est-à-dire s'il s'agit d'une affaire pénale[10] ou civile, selon la gravité ou l'importance de l'affaire, les parties concernées, etc.).

L'expérience pratique durant la pandémie a montré qu'il existe des approches différentes au sein des juridictions et entre elles. Lorsque les procédures ne se déroulent pas en temps utile, c'est-à-dire lorsque tous les participants sont présents au tribunal en même temps (aujourd'hui, des mesures de distanciation sociale sont généralement en place), les procédures se déroulent souvent sur des plateformes de conférence à distance ou, parfois, par conférence téléphonique. Parfois, les procédures sont de nature hybride, certains participants y prenant part en personne et d'autres à distance. Un exemple intéressant de ce dernier cas est la conduite des procès au pénal en Écosse, où tous les participants sont présents en personne au tribunal (avec toutefois des mesures de distanciation sociale), bien qu'avec la possibilité pour un témoin de participer par vidéoconférence, à titre exceptionnel, lorsque cela est nécessaire. Cependant, les jurys écossais sont composés de quinze personnes, ce qui présente des difficultés évidentes pour parvenir à une distanciation sociale. En conséquence, les jurés participent à distance depuis des « centres de jury à distance » (en réalité, des auditoriums dans des cinémas multiplexes qui ont été loués par les services judiciaires écossais), les procédures leur étant transmises, et l'image de chaque juré individuel étant retransmise à un ensemble d'écrans au sein du tribunal.

[10] Voir, par exemple, la déclaration de l'ECBA sur la vidéoconférence dans les affaires pénales (6 septembre 2020), qui aborde la question de savoir dans quel type d'affaires pénales la vidéoconférence pourrait être utilisée.

La situation actuelle constitue également l'occasion d'envisager de nouvelles approches par rapport aux procédures judiciaires traditionnelles en matière civile, tel le Civil Resolution Tribunal (CTR) au Canada, qui est l'un des premiers exemples au monde de règlement en ligne des litiges intégré au système de justice publique[11].

Il est clair qu'il n'y a pas de solution « unique », mais il est tout aussi clair que, quelle que soit la solution adoptée, les principes ci-dessus devront être respectés afin de garantir un procès équitable.

IV. Conclusion

La pandémie de Covid-19 a entraîné des changements rapides des méthodes de travail, changements auxquels les avocats n'échappent pas. La pratique du droit a toujours dépendu de la nécessité de s'engager directement avec les autres : les avocats avec leurs clients, les parties adverses, les confrères négociateurs, les témoins et le tribunal, mais la manière dont ces rencontres ont lieu a, par nécessité, changé. Les avocats, les juges et les systèmes judiciaires n'ont pas toujours été préparés à ce changement, ce qui a inévitablement créé un sentiment d'avancer à tâtons, des faux départs et des changements soudains.

Les avocats et les autres utilisateurs de systèmes à distance ne sont pas les seuls face à ces défis : souvent, le secteur des technologies de l'information, et en particulier les fournisseurs de systèmes de téléconférence, ont dû développer leurs activités et, de ce fait, faire face aux problèmes techniques et juridiques découlant de cette croissance.

Il en est ressorti un paysage en perpétuel mouvement, changeant et inconnu, avec de nouveaux défis soudains, sortis de nulle part, et le besoin d'élaborer des réponses rapides et originales. Ce défi doit être considéré comme une chance remarquable qui peut faire avancer la numérisation de notre société et de nos systèmes judiciaires.

Pourtant, malgré cet état de flux constant, certaines valeurs restent immuables : le respect du secret professionnel/*legal professional privilege*, le respect de la protection des données et des obligations déontologiques et l'exigence primordiale d'un procès équitable.

Dans ces circonstances, bien que les avocats et les systèmes judiciaires ne doivent pas craindre d'adopter de nouvelles méthodes de travail, le défi ne peut pas être relevé aveuglément, sans tenir compte des véritables questions qui doivent être abordées. Les avocats doivent constamment se pencher sur ces questions, en se rappelant que le paysage continue à changer de jour en jour.

C'est dans cet esprit que le présent document vise à fournir, si ce n'est un guide complet du nouveau monde du travail à distance, du moins quelques repères et, espérons-le, des conseils utiles aux personnes perplexes.

[11] https://civilresolutionbc.ca/