EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of the European legal profession

Rue Joseph II, 40/8 - B-1000 Brussels
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

Orientación de CCBE sobre el uso de herramientas de trabajo a distancia por los abogados y los procedimientos judiciales a distancia

27/11/2020

El Consejo de la Abogacía Europea (CCBE), representa a las Abogacías de 32 países miembros y otros 13 países asociados y observadores, y a través de ellos a más de un millón de abogados europeos.

En el presente documento CCBE desea proporcionar a los abogados cierta orientación sobre el uso de instrumentos de trabajo a distancia y sobre la realización de procedimientos judiciales a distancia.

I. Introducción

Se suele decir que los acontecimientos perturbadores pueden a veces dar lugar a nuevas desviaciones radicales de la forma en que se han hecho las cosas en el pasado pero, con frecuencia, pueden simplemente acelerar las tendencias que se han venido desarrollando lentamente durante años.

Esto ha sido particularmente evidente en relación con el efecto que la COVID-19 ha tenido en la forma en que los abogados desempeñan sus funciones e interactúan con los tribunales. Por ejemplo, desde hace varios años en varias jurisdicciones ha aumentado la aceptación de las audiencias judiciales en las que por lo menos uno de los participantes (por ejemplo, los acusados en las audiencias procesales o ciertos testigos en los juicios) ha estado asistiendo a distancia. Sin embargo, hasta que surgieron los problemas derivados de la pandemia de COVID-19, sólo se habían adoptado las medidas más provisionales para la celebración de audiencias a las que se accede totalmente a distancia. Con las restricciones a la circulación impuestas por los reglamentos pertinentes en la mayoría de los países europeos, se han acelerado esas medidas, que antes eran lentas y provisionales.

En muchos aspectos, los sistemas jurídicos han navegado en aguas desconocidas y han utilizado herramientas nuevas. Sin duda, muchos abogados individuales ya estaban familiarizados con herramientas comerciales más antiguas, como las conferencias telefónicas, y también tenían al menos un conocimiento asintiendo con la cabeza de aplicaciones de medios sociales como Facebook Messenger y Skype, pero las conferencias telefónicas tienen limitaciones obvias y lo que puede ser adecuado para el intercambio de bromas sociales y fotos de gatitos lindos no es necesariamente adecuado para la administración de justicia y para la realización de debates confidenciales que están protegidos por el secreto profesional o el privilegio profesional legal.

Hay dos aspectos interrelacionados en el uso de los instrumentos de conferencia a distancia:

- Las consultas y reuniones de los abogados con sus clientes y otros por medios remotos
- Participación a distancia en las audiencias del Tribunal.

Hay un grado de coincidencia en las cuestiones relativas a cada aspecto; pero cada uno de ellos también plantea problemas particulares.

II. El uso de herramientas de trabajo a distancia por parte de los abogados

Hay una clara necesidad de reuniones a distancia, ya sea con clientes, entrevistando a posibles testigos, reuniones de gestión interna, negociaciones con otras partes: lo que normalmente se hacía "cara a cara", en la práctica de un abogado necesita hacerse online. Al principio de la pandemia, ya había una serie de herramientas disponibles, pero el desafío para los proveedores era hacer frente a la ampliación de su y para el usuario era tomar las herramientas que se habían desarrollado para un entorno y desarrollar para otro entorno más difícil, como el de la práctica jurídica bajo el absoluto requisito de confidencialidad.

En este contexto, destacan los siguientes aspectos:

a) Derechos Fundamentales: Las cuestiones relacionadas con los Derechos Fundamentales se plantearán claramente en todos los casos en que existe el Secreto Profesional / Privilegio Profesional Legal, pero puede hacerlo en forma ligeramente diferente maneras. Todas las comunicaciones estarán protegidas por el artículo 8 del CEDH, ya sea en relación con litigios futuros o pendientes, o en relación con negociaciones comerciales, el empleo asesoramiento jurídico, transacciones de propiedad o cualquier otra de las innumerables áreas de un naturaleza en que se puede implicar el asesoramiento jurídico; mientras que también se protegerá en virtud del artículo 6 Comunicaciones del CEDH relacionadas con procedimientos penales o litigios comerciales y de otro tipo. Debe recordarse que los derechos del artículo 8 del CEDH están calificados (aunque ese cliente-abogado comunicaciones gozan de un mayor nivel de protección); considerando que el artículo 6 del CEDH es absoluto.
b) Secreto profesional / Privilegio profesional legal: Esto se aplicará claramente si el cliente es una persona física o jurídica
c) Cumplimiento del Reglamento Europeo de Protección de Datos: Esto afecta a los titulares de los datos que son personas físicas, por lo que claramente se dedicarán a tratar con clientes que son personas físicas. El compromiso del Reglamento cuando el cliente es una persona jurídica puede no parecer tan obvio, pero en la práctica, es probable que exista la necesidad de procesar datos personales relativos a personas físicas, ya sean empleados, clientes, personas con las que se están llevando a cabo negociaciones, etc. Detrás de cada entidad jurídica hay personas físicas

Se trata de esferas de interés que deben revisarse detenidamente al examinar las condiciones de los diversos proveedores de plataformas. Ese análisis suele ser muy directo, entre otras cosas porque las condiciones aplicables pueden no estar necesariamente reunidas en un todo coherente en una sola sección del sitio web correspondiente. A menudo lo que un usuario necesita saber para garantizar el cumplimiento de la RPI y las obligaciones deontológicas puede distribuirse en una serie de documentos - condiciones, políticas de privacidad, anexos, etc., cada uno de los cuales puede estar en secciones completamente diferentes de un sitio web y no necesariamente estar vinculado por hipervínculos o índices cruzados.

A fin de tratar de comprender las cuestiones prácticas que se plantean en relación con la práctica jurídica, CCBE preparó varios documentos de investigación individuales en los que se examinaban las condiciones de varias plataformas de uso frecuente, a fin de compararlas. Como resultado de este ejercicio, surgieron ciertas cuestiones comunes, a saber:

1. ¿Qué grado de accesibilidad y transparencia tienen las condiciones pertinentes?

2. ¿Quién es el controlador de datos?

3. ¿Dónde se almacenan los datos?

4. ¿En qué medida los proveedores de la plataforma venden o comparten datos personales?

5. ¿A qué vigilancia podrían estar expuestos los datos que poseen los proveedores de la plataforma de la nube?

6. ¿Qué seguridad técnica tiene la plataforma?

1. Accesibilidad y transparencia

Se ha comentado anteriormente la dificultad que se plantea con frecuencia al tratar de determinar las condiciones y las políticas de privacidad que son aplicables en un momento dado. A ello se suma la circunstancia de que los proveedores de la plataforma cambian con frecuencia las condiciones y las políticas de privacidad, a veces sacando nuevas ediciones, a veces introduciendo alteraciones no anunciadas en las condiciones existentes que a menudo ni siquiera se destacan, por lo que la única forma de detectar un cambio es mediante una comparación cuidadosa entre el texto más antiguo y el más reciente.

De ello no se desprende necesariamente que la dificultad de acceso se equipare al deseo de ocultar términos desafortunados; por ejemplo, la forma en que se exponen todos los términos pertinentes de Cisco Webex es de una complejidad tan bizantina que incluso el Centro Europeo de Derechos Digitales, en su Informe sobre las políticas de privacidad del vídeo Los Servicios de Conferencias analizaron las condiciones de Cisco como no plenamente conformes con el Reglamento de Protección de Datos, aunque la investigación de CCBE reveló posteriormente que los autores del Informe no habían encontrado una serie de documentos contractuales pertinentes que se encontraban (sin un hipervínculo) en otra sección del sitio web. Si se consideran las condiciones contractuales en su conjunto, Cisco Webex tuvo un mayor cumplimiento del Reglamento de Protección de Datos que el Informe había declarado.

Esta falta de transparencia de los términos y condiciones ha sido comentada por el Supervisor Europeo de Protección de Datos.

En todos los documentos individuales de investigación de CCBE se observó que la falta de claridad no es necesariamente intencional y que, a veces, es desventajosa no sólo para el cliente sino también para el proveedor de la plataforma. Sea como fuere, lo cierto es que los términos y condiciones de las plataformas suelen contener disposiciones y excepciones complejas. Además, muchas de ellas deben complementarse con otros documentos (normalmente también disponibles en la página web) como declaraciones de privacidad y suplementos o acuerdos de procesamiento de datos por defecto.

2. ¿Quién es el controlador de datos?

Los proveedores de plataformas han estado en una especie de curva de aprendizaje a medida que disfrutan de una mayor aceptación de sus plataformas por parte de un número cada vez mayor de usuarios en sectores cada vez más diversos. Algunos proveedores, en particular algunos de los que tienen su sede en Estados Unidos, se han sorprendido al darse cuenta de que existen obligaciones de Reglamento de Protección de Datos que deben cumplir y un nuevo vocabulario jurídico que deben dominar.

Debido a esto, a veces se afirma algo que claramente no es así, por ejemplo, hasta hace poco, Zoom afirmó que nunca podría ser un controlador de datos con respecto a los datos personales que era y Microsoft, aunque adopta un enfoque más matizado, sigue abierto a las críticas por no habiendo analizado completamente las situaciones en las que podría ser realmente un controlador de datos. En particular, el SEPD Investigación sobre el uso de los productos y servicios de Microsoft por parte de las instituciones de la UE, a la que se ha hecho referencia anteriormente, destacó que Microsoft (y otros proveedores) pueden actuar como controladores de datos de maneras que no son siempre transparente, como por ejemplo: los derechos de los proveedores de servicios para modificar los términos de protección de datos unilateralmente; el alcance limitado de las obligaciones de protección de datos de las La falta de fines específicamente definidos para el procesamiento que se produce en virtud de ella.

Mientras que algunas plataformas se consideran controladores de datos (por ejemplo, Kinly y Messenger Video), los términos y condiciones de otras plataformas definen al cliente como el controlador de datos, siendo la plataforma simplemente el procesador. Incluso en este último caso, como se ha observado, las disposiciones de las condiciones, tomadas en su conjunto, pueden funcionar de tal manera y otorgar al proveedor de la plataforma poderes y facultades tan amplios que, en realidad, también actúan como controladores de datos, a pesar de las declaraciones en los términos y condiciones en contrario. Este es el caso, por ejemplo, de Zoom (hasta un cambio reciente en sus términos estándar), Microsoft Teams y Cisco.

3. ¿Dónde se almacenan los datos?

Los términos y condiciones de muchas plataformas no contienen ninguna garantía de que los datos se almacenen en ningún país en particular, ni siquiera dentro de la UE. Esto plantea claramente un problema en relación con el cumplimiento de la normativa sobre el PIB.

En el caso de plataformas como Messenger Video, Skype, Skype for Business, BlueJeans y Cisco, está claro que los datos recogidos en la Unión Europea pueden ser transferidos y almacenados fuera de la UE (principalmente, pero no sólo, en los EE.UU.). En otros casos, no es fácil identificar el Estado en el que se almacenarán los datos porque hay varios centros de datos, como parece ser el caso de Kinly y StarLeaf. Otro ejemplo es el de los equipos de Microsoft, según cuyos términos, dependiendo del país de ubicación del controlador de datos (es decir, el cliente) y del tipo de datos, el lugar de almacenamiento de estos últimos variará. Cabe señalar que, para los controladores de datos de muchos países de la UE, al menos algunos de los datos que controlan se almacenarán fuera de la UE. Esto podría sugerir que la diligencia debida debería incluyen el intento, en la medida de lo posible, de utilizar plataformas cuyos servidores estén alojados en la UE; y que sí que no es posible, tratando de ajustarse a las recomendaciones y decisiones de la Comisión, la EDPB y las autoridades nacionales de protección de datos pertinentes en relación con las transferencias de datos.

El problema se agrava por la circunstancia de que muchos de los proveedores con sede en los EE.UU. confiaron en la autocertificación en el marco del Escudo de Privacidad de la UE-EE.UU. para regularizar esas transferencias de datos, pero la decisión del TJUE en el Schrems II caso de dejar de lado el Escudo de Privacidad ha impedido el uso de este mecanismo. Aunque, la sentencia confirma la continua validez de los contratos estándar Cláusulas, todavía hay una necesidad de vigilancia constante. El TJUE señaló que la necesidad de salvaguardia debe verificarse caso por caso, por lo que el debate sobre la eficacia de tales cláusulas continúa.

4. ¿En qué medida los proveedores de la plataforma venden o comparten datos personales?

Los términos y condiciones de la mayoría de los proveedores de plataformas establecen que, en general, los datos no se venderán ni compartirán, salvo en la medida en que los propios términos y condiciones lo permitan.

A veces, esas declaraciones no deben tomarse al pie de la letra, ya que las secciones de definición dentro de los términos y las condiciones pueden dar significados especialmente definidos a palabras como "vender". Por ejemplo, un proveedor Los términos establecidos que la transferencia de datos a otra persona para el pago de un dinero no cuenta como "venta" si el cesionario tiene términos y condiciones similares a los del proveedor.

Además, dentro de las condiciones, suele haber excepciones en virtud de las cuales los proveedores pueden, de hecho, compartir los datos de los clientes con determinados terceros en determinadas condiciones. Con frecuencia, las consecuencias de esas excepciones no están claras. Por ejemplo, la mayoría de los proveedores de la plataforma están autorizados a compartir datos, de ser necesario, con terceros, como socios comerciales, auditores, asesores jurídicos, filiales y empresas afiliadas. Además, también pueden compartir datos por otras razones, entre ellas el cumplimiento de obligaciones legales o como parte de operaciones corporativas como fusiones o ventas de activos. En algunos casos, la falta de transparencia de las condiciones y la previsibilidad de sus efectos es particularmente problemática, con excepciones amplias y vagas que permiten compartir datos para razones como la aplicación de la política y los acuerdos del proveedor, la puesta en marcha de la empresa del proveedor operaciones o la protección del derecho de propiedad del proveedor de la plataforma.

5. ¿A qué vigilancia podrían estar expuestos los datos en poder de los proveedores de plataformas de nube?

Una preocupación particular bajo esta rúbrica, es el peligro que surge de tantas de las plataformas principales de proveedores que tienen su sede o sus establecimientos en Estados Unidos, donde están sujetos a la jurisdicción de largo plazo de la Ley de Nubes. La Ley de Nubes permite a los tribunales y autoridades de EE.UU. solicitar los datos personales de las empresas de EE.UU. que lo almacenan en servidores de nube dentro de la Unión Europea. La pregunta de la justificación de las transferencias de datos en el contexto de la Ley de Nubes ha sido abordada por el La Junta de Protección de Datos (EDPB) y el Supervisor Europeo de Protección de Datos (SEPD) en una respuesta conjunta a la comisión LIBE del PE. En esta respuesta, consideran que, en caso de una solicitud basada en el Acta de Nubes sin un acuerdo internacional correspondiente al art. 48 RGPD, una transferencia de datos sólo puede justificarse si es necesario para proteger los intereses vitales de los interesados.

6. ¿Con que grado de seguridad técnica cuentan las plataformas?

La seguridad técnica de las plataformas no parece ser un problema importante, pero hay, sin embargo, algunas vulnerabilidades.

Algunas de esas vulnerabilidades se relacionan con los valores predeterminados de la configuración del usuario y pueden abordarse fácilmente si el usuario está atento al riesgo y toma medidas para cambiar la configuración del usuario. Por ejemplo, fue notorio que, al principio del confinamiento, la configuración de usuario por defecto en Zoom se fijó en niveles mínimos de seguridad, permitiendo un acceso muy fácil a los participantes no autorizados, y dando una nueva palabra al idioma inglés: Bombardeo con zoom. Los ajustes fueron capaces de ser establecidos por el usuario para dar mayores niveles de seguridad, pero es notable la cantidad de usuarios que no aplicaron las medidas necesarias. Sin embargo, ser sensible a presiones del mercado, Zoom respondió cambiando su configuración predeterminada para proporcionar mayores niveles de seguridad, y este problema en particular ha desaparecido en gran medida.

Sin embargo, hay otras vulnerabilidades de seguridad que son inherentes a las plataformas y no tan fácilmente dirigido. Esto es particularmente cierto en relación con la naturaleza y el alcance del cifrado proporcionado.

Algunas, pero no todas las plataformas ofrecen cifrado de extremo a extremo. Microsoft, por ejemplo, ofrece encriptación de extremo a extremo, mientras que otras plataformas, como Cisco, ofrecen encriptación estándar por defecto, ofreciendo el cifrado de extremo a extremo sólo como una opción adicional. Se ha informado de que otras plataformas, como Zoom, al principio del bloqueo, proporcionó una "encriptación" que no era ni de extremo a extremo ni en cumplimiento de las normas internacionales sobre encriptación, aunque eso es algo que Zoom ha desde que se abordó.

7. ¿Existen impedimentos para la disponibilidad de los recursos?

Las Condiciones Generales suelen contener cláusulas de elección de ley y de jurisdicción exclusiva. Vale la pena teniendo en cuenta que éstas (en particular la última) pueden presentar obstáculos prácticos para la obtención de remedios. Esto es especialmente problemático ya que muchos proveedores tienen cláusulas que confieren exclusividad en un estado particular o la jurisdicción federal de los Estados Unidos (y, a veces, en un tribunal de una ciudad determinada), aunque algunos, en particular Cisco, prevén la jurisdicción en al menos una jurisdicción europea.

<u>Conclusiones sobre el uso de instrumentos de trabajo a distancia por los abogados</u>

Como se desprende del análisis anterior, es necesario que los abogados lean, comprendan y revisen periódicamente las condiciones de las plataformas que utilizan para asegurarse de que respetan debidamente sus obligaciones de protección de datos y deontológicas. Las diversas plataformas ofrecen diferentes normas de fiabilidad, solidez, experiencia del usuario y similares, y puede haber una tendencia natural a elegir la que dé, subjetivamente, la mejor experiencia y las características más útiles. Eso es en gran parte una cuestión de gusto, pero, en el análisis final, la elección de un instrumento apropiado depende no sólo de esos factores, sino también de un examen cuidadoso de el gran invisible - el cumplimiento del PIBR, la protección de la confidencialidad, la robustez de los términos y condiciones desde el punto de vista del usuario. Además, como se desprende del análisis

anterior, se trata de una revisión ejercicio que no puede realizarse una sola vez sino que debe realizarse constantemente.

III. Procedimientos judiciales remotos

Diferentes tribunales en diferentes jurisdicciones llevan a cabo procedimientos remotos utilizando diferentes plataformas. Aunque siguen existiendo las mismas cuestiones que se han examinado anteriormente, es probable que en la práctica sean de menor preocupación a los abogados, ya que es el Tribunal el que probablemente sea el Controlador de Datos, en lugar de los abogados. En cualquier caso, los procedimientos judiciales suelen celebrarse en público y, en algunas jurisdicciones, una vez que los documentos son referidos en la corte, se convierten en documentos públicos. Además, también puede ser que en algunas jurisdicciones, el acto de revelarlos al juez y a la otra parte significará que el Secreto Profesional del abogado ya no se les aplicará, mientras que en otras jurisdicciones el acto de revelar documentos al juez y a la otra parte no afecta al deber de los abogados de observar el Secreto Profesional en relación con estos documentos.

Sin embargo, esto no significa que los Colegios de Abogados y los abogados individuales puedan ignorar las cuestiones de privacidad y protección de datos. Se puede dar un ejemplo real de Inglaterra y Gales donde, en una etapa temprana de la pandemia, hubo una propuesta del Servicio de Tribunales de que los procedimientos ante el Tribunal de Familia de Inglaterra y Gales procedieran por medio de Zoom. Esto era especialmente preocupante, ya que los datos derivados de esos procedimientos serán a menudo categorías especiales de datos personales, y esos procedimientos se celebrarán normalmente en privado. Por consiguiente, era necesario señalar a la administración del tribunal estas preocupaciones particulares, así como las genéricas que se habían expresado acerca de la plataforma Zoom en el estado en que se encontraba en ese momento.

Es más probable que la preocupación cotidiana sea la cuestión de la realización de un juicio justo conforme al artículo 6 del Convenio Europeo de Derechos Humanos. Cabe destacar la exigencia de que haya canales privados seguros paralelos accesibles para los respectivos clientes y sus equipos jurídicos.

Las pruebas anecdóticas sugieren que la mayoría de los tribunales no están proporcionando esta facilidad, pero que los equipos están haciendo sus propios arreglos ad hoc (plataformas separadas; correo electrónico; grupos de chat en varias plataformas, etc.) Se plantea la cuestión de si esto es jurídicamente adecuado para garantizar un juicio justo, especialmente si hay diferentes niveles de conocimientos técnicos en los equipos contrarios, y problemas prácticos en cuanto a cómo es mejor usar esos canales paralelos.

Lo que es más significativo, una vez que los abogados proporcionan sus propios canales, eso vuelve a despertar las mismas cuestiones que surgen en relación con las reuniones a distancia como se ha mencionado anteriormente. Por ejemplo, si un abogado estableciera un canal paralelo utilizando, por ejemplo, un chat de grupo en el Facebook Messenger, entonces el chat (que estaría muy sujeto al PS/LPP) sería retenido por Facebook en sus servidores y sometido a vigilancia en virtud de la Ley de la Nube. Tal vez el medio utilizado podría ser What's App que es, sin duda, técnicamente más seguro. Sin embargo, el problema sigue siendo que el medio utilizado para tal canal paralelo puede no ser uno que sería utilizado por el abogado para otros negocios a distancia; lo que no excusa al abogado de tener que realizar, en relación con ese canal, el mismo tipo de diligencia debida que ha que se empleará para considerar qué instalación de conferencias a distancia se utilizará.

Habría otras cuestiones que no son de naturaleza puramente informática, inherentes a los procedimientos a distancia. Para ejemplo, en relación con la igualdad de armas: la desventaja para las partes que no tienen acceso a la tecnología de la información, el efecto de los pobres velocidad de Internet, la dificultad de un juez para evaluar eficazmente la credibilidad de un testigo sin viendo el testigo en carne y hueso, los problemas de seguridad de las conexiones remotas (¿cómo se puede saber si, metafórica o literalmente, el hombre que sostiene la cámara frente al testigo no es también sosteniendo un arma?). Ciertamente, estos argumentos no pueden ser totalmente excluidos en los procedimientos reales: también puede que las partes que carecen de acceso a la tecnología de la información también carecen de los medios para prestar asistencia jurídica y que un testigo puede ser influenciado de otras maneras antes de una audiencia judicial, por ejemplo, mediante amenazas. No obstante, necesitan ser considerados.

Estos y otros asuntos se examinaron en un documento de CCBE sobre el uso de la videoconferencia en casos penales y civiles, que se basó en la posición de CCBE sobre las propuestas de modificación de las normas de notificación de documentos y de obtención de pruebas en asuntos civiles y comerciales (19/10/2018). También cabe destacar aquí las siguientes observaciones genéricas formuladas en ese documento, que son pertinentes para los procedimientos tanto en materia civil como, aún más, en materia penal y civil:

- Antes de llegar a una determinación final sobre qué programa de videoconferencia ("VC") utilizar, los tribunales y las autoridades judiciales deberían poner en práctica su sistema de VC utilizando un programa piloto que puedan evaluar y modificar. Los tribunales deberían establecer un sistema en el que, después de una videoconferencia, reciban información de todos los participantes sobre la organización de la videoconferencia a fin de seguir mejorando su sistema de videoconferencia. Además, los tribunales deberían proporcionar una formación estructurada a los jueces y a cualquier persona que vaya a manejar el equipo de la CV durante la audiencia, así como garantizar la formación adecuada y la disponibilidad del personal de TI. También deberían compartir entre sí las mejores prácticas de la videoconferencia a fin de reducir los costos y aumentar la eficiencia.
- Es necesario contar con planes de contingencia para hacer frente con eficacia a cuestiones como el descenso o malas conexiones durante la sesión de VC.
- En los casos transfronterizos, en particular en los que las partes pueden no ser nativas y estarán sujetas a diferentes influencias culturales, el juez tal vez no pueda examinar tan fácilmente los matices del aspecto y las respuestas de las partes a través de un enlace de vídeo. Además, los jueces podrían tener tendencia a hacer menos preguntas y ser menos propensos a interrumpir un argumento, lo que podría no ser un resultado beneficioso para las partes. Por lo tanto, es importante que se adopten las disposiciones técnicas adecuadas para garantizar en la medida de lo posible una experiencia auditiva realista que incluya la plena comunicación e interacción de todas las partes en el procedimiento con el testigo u otra persona que está siendo interrogado. La videoconferencia a nivel de consumidor los servicios, como Skype o FaceTime, son inadecuados en este sentido.
- En algunas jurisdicciones, el uso de la videoconferencia podría estar sujeto a la aprobación de las partes. Relevante las preguntas son así: ¿Es necesario solicitar el consentimiento de las partes para participar en una VC? ¿En qué condiciones pueden las partes rechazar una VC? ¿Es necesario que esté presente un asesor jurídico o consultado si las partes consienten o rechazan?
- El tribunal o la autoridad judicial debe notificar los datos a las partes, incluidos sus abogados, el tiempo, el lugar y las condiciones de participación en la VC. Se debe avisar con suficiente

antelación dado. En este contexto, ¿cuánto tiempo debe durar la notificación para que se considere suficiente?

- Hay que hacer arreglos para que el abogado pueda participar en la VC. El abogado debería poder sentarse junto a su cliente. Si esto no es posible, los arreglos para que el abogado pueda participar en la VC desde otro lugar.
- Cuando las normas locales exigen que un abogado participante aporte pruebas de su identidad y derecho a comparecer, el abogado debe estar habilitado para hacerlo, a distancia si es necesario.
- El tribunal o la autoridad judicial pertinente debe dar instrucciones al abogado en cuanto al procedimiento que debe seguirse para presentar documentos u otro material durante el VC. Es necesario hacer arreglos para asegurar que todos los participantes en la CV puedan ver cualquier material que se presente durante el VC.
- En los casos en que los documentos deban ser mostrados a un testigo, eso debe hacerse a través de una persona independiente que esté presente con ellos (secretario judicial o similar) que pueda asegurar (por ejemplo, del punto de vista de la fiscalía) que están mirando la página correcta y (desde el punto de vista de la defensa punto de vista) también se aseguran de que no están mirando otros documentos, especialmente no en documentos que no han sido revelados a la defensa o a otras partes.

Estas preocupaciones son pertinentes tanto con respecto a los procedimientos penales como a los civiles. Sin embargo, la respuesta a la pregunta de si, en un caso concreto, las actuaciones a distancia pueden considerarse una forma adecuada de llevar a cabo las actuaciones puede diferir ciertamente según la naturaleza del caso (es decir, si se trata de un procedimiento penal o un caso civil; la gravedad o importancia del caso, las partes involucradas, etc.).

La experiencia práctica durante la pandemia ha demostrado que hay diferentes enfoques tanto dentro de las jurisdicciones como entre ellas. Cuando los procedimientos no se llevan a cabo en la forma en que se permite que todos los participantes estén presentes en el tribunal al mismo tiempo (ahora generalmente con medidas de distanciamiento social que se encuentran en el lugar), las actuaciones suelen tener lugar en plataformas de conferencias a distancia, u ocasionalmente, por conferencia telefónica. A veces las actuaciones son de naturaleza híbrida, con algunos participantes que participan en persona y otros a distancia. Un ejemplo interesante de esto último es la conducta de los juicios penales en Escocia, en los que todos los participantes están presentes en el tribunal en persona, (aunque con distanciamiento social) aunque con la posibilidad de que un testigo participe por videoconferencia donde, excepcionalmente, eso es necesario. Sin embargo, los jurados escoceses están formados por quince personas, y eso presenta desafíos obvios para lograr el distanciamiento social. En consecuencia, los jurados participan a distancia de "centros de jurado remotos" (en realidad, auditorios en cines múltiples que han sido alquilados por los escoceses con los procedimientos transmitidos a ellos, y la imagen de cada uno de los jurados transmitido a un banco de pantallas en la corte.

La situación actual nos da también la oportunidad de considerar nuevos enfoques de la corte tradicional procedimientos en asuntos civiles como el Tribunal de Resolución Civil del Canadá, que es

uno de los más importantes del mundo y de los primeros ejemplos de resolución de controversias en línea (ODR) que se han incorporado al sistema de justicia pública.

Está claro que no existe una solución "de talla única"; pero lo que también está claro es que, sea cual sea la solución que se adopte, será necesario seguir los principios antes mencionados para ofrecer un juicio justo.

IV Conclusiones

La pandemia de COVID-19 ha forzado cambios rápidos en la forma en que todos trabajamos, y los abogados no están exentos de estos cambios. La práctica del derecho siempre ha dependido de la necesidad de relacionarse directamente con los demás: los abogados con sus clientes, con sus oponentes, sus contrapartes negociadoras, los testigos y el tribunal, pero la forma en que esos encuentros han tenido lugar ha cambiado por necesidad. No siempre ha sido un cambio para el que los abogados, los jueces y los sistemas de justicia se han preparado, e inevitablemente ha habido una sensación del camino, falsos comienzos y cambios repentinos.

Los abogados y otros usuarios de sistemas remotos no son los únicos que se enfrentan a estos retos, y a menudo la industria de la tecnología de la información y, en particular, los proveedores de sistemas de conferencias a distancia han tenido que ampliar sus negocios y, al hacerlo, hacer frente a las cuestiones técnicas y jurídicas que se derivan de ese crecimiento.

El resultado ha sido un panorama en constante movimiento, cambiante y desconocido, con nuevos desafíos repentinos que surgen de la nada, y la necesidad de elaborar respuestas rápidas y novedosas. Este desafío debe considerarse como una gran oportunidad que puede impulsar la digitalización de nuestra sociedad y nuestros sistemas judiciales.

Sin embargo, a pesar de este constante estado de cambio, algunos valores siguen siendo inalterables: el respeto del secreto profesional, el cumplimiento de las obligaciones de protección de datos y deontológicas y el requisito general de proporcionar un juicio justo.

En estas circunstancias, aunque los abogados y los sistemas de justicia no deben temer afrontar el reto de trabajar de nuevas maneras, esto no es algo que pueda hacerse a ciegas, sin prestar atención a las cuestiones muy reales que deben abordarse. Los abogados requieren constantemente estar abordando estas cuestiones, recordando que el panorama sigue cambiando día a día.

Es con todo esto muy en mente que este documento trata de proporcionar, sino una guía completa para el nuevo mundo del trabajo a distancia, luego al menos unos pocos carteles de señalización y alguna guía esperanzadoramente útil a los perplejos.