Posición de la CES sobre los acuerdos de comercio digital de la UE con terceros países

Adoptada en la reunión del Comité Ejecutivo de 10-11 de diciembre 2024

Según la Comisión Europea, el comercio digital abarca el comercio de bienes y servicios posibilitado por internet y otras tecnologías de la información y la comunicación. Esto incluye bienes o servicios pedidos en línea que luego se entregan en casa o a través de internet, como aplicaciones en teléfonos inteligentes y ordenadores; uso de tecnologías como las utilizadas para el seguimiento en tiempo real; transferencia de datos a través de las fronteras (por ejemplo, datos almacenados en la nube cuando se trabaja en línea).

La UE es el mayor exportador mundial de servicios, la mitad de los cuales son servicios digitales. Así, la UE tiene una gran responsabilidad en el desarrollo sostenible y la salvaguarda de los intereses públicos de este sector Con este fin, la UE ha estado negociando Acuerdos autónomos de Comercio Digital (DTA, por sus siglas en inglés), especialmente cuando los acuerdos comerciales existentes con países socios no incluyen capítulos de comercio digital. Con los DTA, la UE no sólo pretende abrir los mercados y mejorar el acceso al comercio electrónico, sino también garantizar la protección de los consumidores de la UE, protegiendo sus datos y su privacidad, algo que la Comisión sostiene que no es negociable, pero el Supervisor Europeo de Protección de Datos ha expresado su preocupación por que en la práctica no sea así y que a veces dichas protecciones se negocian.

En el verano de 2024, la UE y Singapur celebraron un DTA que complementa el actual ALC UE-Singapur. Con este acuerdo adicional, la UE aspira a establecer una norma mundial para las normas del comercio digital y los flujos de datos transfronterizos. El acuerdo podría presentarse al Parlamento Europeo para su ratificación en enero de 2025. La UE también está negociando acuerdos similares con Corea del Sur, Filipinas y Tailandia.

Esta posición establece los principios rectores de la CES con los que se medirán este y futuros DTA para representar un patrón oro. Algunos de estos principios, en su caso, se extenderían también a las negociaciones sobre comercio electrónico en el marco de la OMC. Esta posición complementa las resoluciones existentes sobre comercio y otras áreas políticas relevantes.

Derecho a regular y espacio de política económica: Los DTA deben preservar y no socavar el espacio político para adoptar medidas reguladoras y de otro tipo, incluido a través del diálogo social y la negociación colectiva, para hacer frente a los nuevos retos de la economía digital, incluyendo la protección de los datos de salud pública, el control público y la resistencia de la infraestructura digital, la creación de valor regional, la IA y anclando el principio de «control humano». Los acuerdos de comercio digital no deben afectar negativamente a la capacidad de la UE para hacer cumplir su propia legislación

digital y de los Estados miembros para ir más allá de las normas mínimas de la UE.

Derechos de los trabajadores: Los acuerdos de comercio digital no deben impedir la aplicación de los derechos de las personas trabajadoras ni la mejora de las condiciones de trabajo. Para ello, los DTA no deben prohibir la obligación de que las empresas tengan presencia legal y/o física en el territorio de las partes del acuerdo. Los DTA no deben impedir que los trabajadores y trabajadoras reclamen un derecho sobre los datos y el valor económico que producen: las normas comerciales no deben cimentar la propiedad exclusiva de las empresas sobre los datos recopilados. También debe garantizarse la participación de las y los trabajadores en la gobernanza de los datos. Por otra parte, las empresas digitales que abusan de los derechos de las trabajadoras y trabajadores no deben ser recompensadas con la liberalización del comercio y mayores derechos de acceso al mercado a través de los DTA.

Flujos de datos y protección: la UE dispone de cláusulas modelo sobre flujos de datos. Sin embargo, en los DTA, la UE a veces se adapta a las necesidades del socio: esto puede dar lugar a la dilución de la protección de los derechos de las personas trabajadoras, incluida la privacidad de los datos, aumenta la inseguridad jurídica, así como la exposición a disputas comerciales sobre derechos digitales. Esto debe evitarse: la UE debe limitarse a conceder decisiones de adecuación de datos, ya que se trata de medidas unilaterales que pueden retirarse en cualquier momento. Los DTA no deben debilitar al Supervisor Europeo de Protección de Datos ni a las autoridades nacionales. Los acuerdos comerciales no deben establecer las normas para el flujo transfronterizo de datos sin garantías de que el RGPD de la UE siempre tendrá prioridad sobre los términos comerciales. Los intereses públicos y la protección de datos siempre deben tener prioridad sobre los intereses comerciales ofensivos.

El acceso al código fuente no se debe prohibir a las autoridades públicas, que podrían necesitar este acceso para casos legales concretos, como litigios de propiedad intelectual, o por razones más generales, como garantizar la estabilidad económica o investigar posibles sesgos y prácticas fraudulentas. La capacidad de los organismos reguladores para garantizar que las empresas cumplen los requisitos legales podría verse mermada con una prohibición general del acceso al código fuente. Además, debe garantizarse el libre acceso al código fuente antes de la implementación de sistemas de IA en el lugar de trabajo. Bloquear el acceso al código fuente, si se consagra en los DTA, socavaría la transparencia y el equilibrio de poderes necesarios para evitar el uso indebido de la gestión algorítmica.

Impuestos a las grandes tecnológicas: ninguna cláusula de los DTA debe impedir a las partes del acuerdo, directa o indirectamente, gravar los beneficios de las grandes tecnológicas. Una cosa es prohibir los derechos de aduana sobre las transmisiones electrónicas, como los intercambios de correos electrónicos, y otra impedir que un Estado introduzca un impuesto sobre los servicios digitales o aumente el nivel existente del impuesto de sociedades. Las prohibiciones a la localización de datos también dificultan la capacidad de las autoridades para evaluar los beneficios empresariales, por ejemplo impidiendo que se exija almacenar los datos contables localmente, y corren el riesgo de socavar la Directiva de información pública país por país de la UE.

Servicios públicos y digitalización: Los DTA no deben conducir a la privatización de los

servicios públicos, ni siquiera a través de asociaciones cada vez más estrechas entre el sector público y el privado. Además, existen riesgos de socavar los valores públicos y la seguridad nacional en algunos casos; de aumentar la dependencia de ciertos proveedores dominantes en otros; de impedir la supervisión de la toma de decisiones algorítmicas para determinar el acceso a las prestaciones y otros servicios públicos; de «pagar dos veces» por lo que son nuestros propios datos como ciudadanos y ciudadanas y pacientes. Del mismo modo, los DTA no deberían atrincherarse en el uso de la seguridad nacional o el orden público para diluir o impedir una mayor regulación y escrutinio público (como ocurrió con el convenio marco del Consejo de Europa sobre IA). La CES considera que los servicios públicos y las infraestructuras deben quedar al margen de las negociaciones comerciales y de inversión, lo que también se aplica a los DTA, y que, como mínimo, los datos recogidos a través de la prestación de servicios públicos deben seguir siendo de titularidad pública.