Las tres sendas hacia la privacidad

The Three Paths to Privacy

Pilar Vargas Martínez
Profesora sustituta de Derecho Internacional
Universidad Complutense de Madrid

Resumen:

En materia de gobernanza del dato, el análisis comparado de las políticas seguidas por la Unión Europea, los Estados Unidos y la República Popular China puede representarse a través de tres metáforas históricas con lógicas regulatorias bien diferenciadas: el Camino de Santiago, la Ruta 66 y la Ruta de la Seda. El Camino de Santiago, caracterizado por ser una red supranacional de protección, hospitalidad y reglas comunes refleja el enfoque de la Unión Europea, donde la privacidad se configura como un derecho fundamental. Así, el peregrino medieval y el ciudadano digital comparten un marco que busca protegerlos durante su tránsito, lo que asegura que la movilidad (física o digital) se mantenga como un elemento central de la cohesión y la identidad europeas. Por su parte, la Ruta 66 estadounidense simbolizó un modo de entender la movilidad asociado a la libertad individual y al espíritu empresarial. En cambio, en la Ruta 66 las normas eran mínimas y el propio conductor asumía la responsabilidad de gestionar riesgos y oportunidades. Esta lógica es coherente con la tradición regulatoria estadounidense, caracterizada por una intervención estatal limitada y una marcada preferencia por la autorregulación y el libre mercado. La Ruta de la Seda, al ser una vía histórica de intercambio controlado y herramienta de proyección estratégica del poder imperial, permite entender el modelo chino, basado en la soberanía digital, la centralidad del Estado y la primacía de la seguridad nacional. Su legislación articula un régimen que combina protección formal del individuo con un marcado autoritarismo. En conjunto, estos tres modelos revelan un panorama global fragmentado, donde conviven enfoques garantistas, liberal-mercantilistas y soberanistas, lo que produce tensiones estructurales en la gobernanza del dato y en su viabilidad regulatoria.

Palabras clave:

Protección de datos, privacidad, Estados Unidos, Unión Europea, China.

Abstract:

In the field of data governance, a comparative analysis of the policies pursued by the European Union, the United States, and the People's Republic of China can be represented through three historical metaphors with clearly differentiated regulatory logics: the Camino de Santiago, Route 66, and the Silk Road. The Camino de Santiago, characterized as a supranational network of protection, hospitality, and shared rules, reflects the approach of the European Union, where privacy is conceived as a fundamental right. In this sense, the medieval pilgrim and the digital citizen share a framework designed to protect them during their journey, ensuring that mobility (whether physical or digital) remains a central element of European cohesion and identity. By contrast, the American Route 66 symbolized a conception of mobility associated with individual freedom and entrepreneurial spirit. Along Route 66, rules were minimal and the driver assumed responsibility for managing risks and opportunities. This logic is consistent with the U.S. regulatory tradition, characterized by limited state intervention and a strong preference for self-regulation and the free market. The Silk Road, as a historical route of controlled exchange and a tool for projecting imperial strategic power, helps explain the Chinese model, which is based on digital sovereignty, the centrality of the state, and the primacy of national security. Chinese legislation establishes a regime that combines formal protection of the individual with a pronounced authoritarian dimension. Taken together, these three models reveal a fragmented global landscape in which rights-based, liberal–market-oriented, and sovereignist approaches coexist, generating structural tensions in data governance and in its regulatory viability.

Keywords:

Data protection, privacy, United States, European Union, China.

1. Las tres sendas hacia la privacidad

La Unión Europea (UE), los Estados Unidos (EE. UU.) y la República Popular China (China) son los tres principales actores en el comercio mundial de servicios, incluidos los servicios digitales. De hecho, la UE y los EE.UU. son los principales socios comerciales en la exportación e importación de servicios digitales. En 2019, los servicios digitales representaron una parte muy significativa del comercio de servicios de EE.UU,[1] donde aproximadamente el 59 % de todas las exportaciones de servicios y el 50 % de sus importaciones de servicios estaban relacionados con servicios habilitados digitalmente, lo que representó también una gran mayoría del superávit mundial estadounidense en comercio de servicios[2].

En la UE, los servicios digitales constituyen una parte importante del comercio de servicios del bloque con terceros países. La UE es uno de los mayores exportadores e importadores de servicios del mundo, con alrededor del 25 % del comercio mundial de servicios, y los servicios digitales se encuentran entre los segmentos más dinámicos de este sector[3]. En cuanto a las exportaciones de servicios de la UE, constituyen uno de los principales destinos, al representar cerca de una quinta parte de las exportaciones totales de servicios de la UE en 2023. En sentido inverso, se estima que las exportaciones de servicios digitales de los EE.UU. con destino la UE representan entre un 25 % y un 30 % del total de sus exportaciones en servicios digitales.

Por su parte, China ha crecido rápidamente como actor global en comercio, especialmente en bienes manufacturados; sin embargo, a diferencia del sector de productos digitales, en servicios digitales persiste una participación menor en comparación con la UE y EE. UU. En consecuencia, los datos disponibles muestran que el comercio de servicios de China es aún más limitado y, del mismo modo, sus exportaciones de servicios digitales exponen una fracción menor del total mundial comparado con los líderes transatlánticos[4].

En ese orden de ideas, resulta evidente que el comercio digital se ha convertido en un elemento central de las relaciones económicas y comerciales globales. A pesar de ello, han existido presiones políticas (especialmente desde la UE) para restringir el flujo transfronterizo de datos entre los principales bloques y, con este, de numerosas operaciones comerciales, lo que argumenta el mantenimiento de estándares de privacidad y explica, por defecto, su creciente intervención restrictiva en el pasado. A su vez, los EE. UU. han liderado recientemente una ofensiva en el sentido inverso, que podría haber calado en el regulador europeo. Aún así, cabe esgrimir que la contraposición absoluta entre privacidad y comercio resulta engañosa.

En ese sentido, se debe partir de la base de que, si bien el derecho humano a la privacidad está universalmente reconocido, su alcance sobre la protección de datos personales no cuenta con una lectura uniforme, dado que mientras en algunos lugares constituye un derecho fundamental, en otros carece de esta consideración. A la luz de este contexto, se arguye que regulación nacional de la protección de la privacidad y de los datos personales, como la de cualquier objetivo legítimo de interés público nacional, está ligada a los valores constitucionales y éticos que persiguen los

[1] Según diferentes informes del BEA y estudios especializados sobre comercio digital los Servicios habilitados digitalmente (*digitally deliverable services*): Representan aprox. el 60 % de todas las exportaciones de servicios de EE. UU; Representan aprox. el 52 % de todas las importaciones de servicios; y Generan más del 75 % del superávit total estadounidense en comercio de servicios. Esto significa que el superávit de EE. UU. en servicios proviene abrumadoramente del sector digital, no del sector industrial.

[2] *The Transatlantic Economy 2021: Digital Acceleration*, The Transatlantic Economy, 2021, https://transatlanticrelations.org/wp-content/uploads/2021/03/TA-economy-2021_CH4.pdf?utm_source=chatgpt.com

[3] Comisión Europea, "Servicios – estadísticas," acceso el 8 de marzo de 2026, https://trade.ec.europa.eu/access-to-markets/en/content/services-statistics?utm_source=chatgpt.com

[4] Jacques Delors Institute, *Europe in the World: Mapping the EU's Digital Trade—A Global Leader Hidden in Plain Sight?* (París: Jacques Delors Institute, 2023).

diferentes Estados[5].

Ahora bien, en EE. UU. no existe una normativa transversal específica para la protección de datos, sino normativas sectoriales al respecto. Sobre esto, la Constitución no menciona este derecho concreto en torno a la protección de los datos frente al uso que los responsables de su tratamiento hacen de ellos[6].

En efecto, más allá del reconocimiento por el Tribunal Supremo del derecho a la intimidad en el ámbito del derecho penal y en el de la salud reproductiva, se evidencia que la salvaguarda de la información personal de los estadounidenses reside, en gran medida, en la ley de protección del consumidor. En este sentido, no puede perderse de vista que, en sistemas jurídicos del entorno europeo, los datos personales y su protección se conciben como un derecho fundamental en sí mismo[7] mientras que, en otros, como los EE. UU., aunque se sitúe en el marco del respeto a la privacidad del individuo como derecho fundamental, se asocia esencialmente a la protección de los consumidores[8]. De tal modo, esto puede traducirse en distintas consideraciones de los datos personales; es decir, como un derecho en la UE frente a su catalogación como una mercancía o el propio objeto de una transacción económica en los EE.UU.

Sin embargo, aunque se discuta esta caracterización, quien recogió los datos puede, salvo en algunos ámbitos, disponer de ellos prácticamente como sí de un bien más se tratara[9]. De este modo, resulta evidente que reúnen cualidades distintas de las mercancías tradicionales al estar directamente vinculados con aspectos personales de los individuos. En consecuencia, su mercantilización, que busca obtener rendimientos económicos, ha dado lugar a un "capitalismo de vigilancia" (*surveillance capitalism*). Así, desde el punto de vista de las transferencias internacionales de datos, se advierte que la legislación sectorial estadounidense no contiene restricciones generales. Asimismo, la amplia legislación en materia de privacidad considerada recientemente tampoco preveía un cambio fundamental de este enfoque de "*laissez-faire*", y parece poco probable que se efectúe en el futuro.

Por el contrario, el Reglamento general de protección de datos (RGPD)[10] de la UE condiciona los flujos de datos de carácter personal desde el territorio de la UE a la existencia de garantías de privacidad que se desplacen con los datos hacia su lugar destino. Por lo tanto, si la Comisión Europea ha decidido que un tercer país concreto ofrece un nivel de protección "adecuado", los datos pueden circular libremente hacia este desde el territorio de la UE sin formalidades adicionales. Para todos los demás destinos, las salvaguardas deben incluirse en los contratos comerciales individuales de transferencia de datos (como cláusulas contractuales tipo).

En ese sentido, la UE ha aumentado gradualmente el número de decisiones de adecuación que ha emitido, lo que permite flujos de datos sin restricciones a los Estados favorecidos por estas; no obstante, los efectos en el comercio digital mundial siguen siendo relativamente modestos, dado que se han emitido 15 decisiones unilaterales de adecuación en 25 años de esfuerzos[11]. Asimismo,

[5] Carmen Otero García-Castrillón, *Protección de datos en la economía digital una aproximación desde la regulación del comercio internacional* (Pamplona: Thomson Reuters Aranzadi, 2021), 74.

[6] Solamente tendría relevancia la Cuarta Enmienda de la Constitución en lo que concierne a la recopilación y el uso de información de datos personales por parte de organismos gubernamentales.

[7] Paul Schwartz y Karl-Nikolaus Peifer, en "Structuring International Data Privacy Law", *International Data Privacy Law 9*, no. 1 (2019): 7-21, señalan "European data protection law is strongly anchored at the constitutional level. Its goal is to protect individuals from risks to personhood caused by the processing of personal data". En este sentido, se hacen eco de cómo Tribunal Constitucional Federal alemán -casos *Census* (1983) e IT *Privacy* (2008)- han cumplido un papel destacado en la conceptualización europea de la privacidad de los datos, al destacar cómo el tratamiento de datos de carácter personal puede amenazar la autonomía de la toma de decisiones individual y socavar "una comunidad democrática libre basada en la capacidad de sus ciudadanos para actuar y participar". El resultado es el concepto de "derecho a la autodeterminación informativa", una idea que la legislación europea sobre privacidad de datos ha adoptado buscando prevenir los riesgos causados por el tratamiento de datos personales.

[8] Otero García-Castrillón. "Protección…", 35

[9] *Ibid*, 48

[10] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), DOUE L 119, 4 de mayo de 2016, 1–88.

[11] Andorra, Argentina, Canadá (solo para organizaciones comerciales), Islas Feroe, Guernsey, Israel, Isla de Man, Japón, Jersey, Nueva Zelanda, República de Corea del Sur, Suiza, Reino Unido, EE. UU. (bajo el marco EU-US Data Privacy Framework) y Uruguay. Serían 16 si se incluye la de la Organización Europea de Patentes, de menor relevancia en el contexto específico que se expone.

se han celebrado escasos acuerdos de comercio digital[12]. En efecto, la UE -por número de acuerdos de comercio digital firmados- se sitúa a la cola de sus grandes competidores en el comercio digital. Como resultado, se observa que una gran proporción de las transferencias de datos de carácter personal entre la UE y el resto del mundo requieren la meticulosa y económicamente ineficiente inclusión de cláusulas contractuales tipo en las contrataciones de servicios que implican de transferencia de datos.

Aunado a esto, se expone que, en la relación entre la UE y EE. UU. se han alcanzado notables progresos para la estabilización de las transferencias de datos. En primer lugar, se encuentra el acuerdo *Data Privacy Framework*[13] -que sustituye al antiguo *Privacy Shield*-; en segundo lugar, está la firma, tanto de la UE como de los EE.UU., de la Declaración de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre el acceso de los gobiernos a los datos de carácter personal en poder de responsables o encargados del tratamiento del sector privado[14]. Sin embargo, para establecer un marco jurídico más estable entre ambas potencias aún queda margen para profundizar en la negociación bilateral y en la búsqueda de un acuerdo de comercio digital específico para cada sector, utilizando para ello el Consejo de Comercio y Tecnología (TTC), que podría trabajar para un entendimiento común sobre la evaluación de riesgos de transferencias internacionales de datos de carácter personal (TIAS por sus siglas en inglés *Transfer impact assessment*).

A la luz de lo expuesto, un pertinente punto de inicio para encontrar un entendimiento en el largo plazo entre la UE y los EE. UU. puede ser el planteamiento común -ya hoy compartido en cierta medida por europeos y estadounidenses y presente en una serie de instrumentos jurídicos internacionales sobre flujos de datos- sobre la responsabilidad proactiva de las entidades que tratan los datos personales de los individuos. En efecto, se plantea que estas entidades deben evaluar los riesgos asociados al tratamiento de datos que realicen, establecer políticas, procedimientos y mecanismos internos con el objeto de gestionarlos de forma segura y, en su caso, aportar pruebas de su cumplimiento a las autoridades de supervisión en la materia, así como a los interesados que ejerzan determinados derechos de protección de datos de carácter personal.

Al respecto, varias autoridades europeas de protección de datos han elaborado guías al efecto para los responsables y encargados del tratamiento. De tal modo, el objetivo de esta estrategia es doble: por un lado, promueve que estos evalúen los riesgos derivados de las transferencias internacionales de datos y de la potencial supervisión por parte de gobiernos extranjeros. Lo anterior se denomina TIA, tal y como se ha indicado. Por otro lado, fomentan el establecimiento de salvaguardias correspondientes mediante cláusulas contractuales tipo[15]. Por su parte, los EE. UU. no han adoptado un enfoque de diligencia equivalente al europeo, a pesar de los intentos infructuosos en este sentido.[16] En cambio, China ha establecido un sistema enfocado en la seguridad nacional antagónico a la filosofía occidental de un internet libre y, en consecuencia, de la liberalización de los flujos de datos.

En todo caso, esta situación revela cómo las distintas visiones de la privacidad -como un derecho del consumidor en los EE. UU. y como un derecho fundamental en la UE- inciden en el ámbito del comercio internacional. Tal vez por esta razón los EE.UU.[17] solían encabezar, hasta muy recientemente[18] tanto a escala bilateral como regional, la firma de acuerdos internacionales para la liberalización de intercambios comerciales en los que ha empezado a incorporarse la protección

[12] La UE ha concluido acuerdos con capítulos de comercio digital con Canadá, Singapur, Vietnam, Japón, Reino Unido, México, Chile, Mercosur y Nueva Zelanda (algunos de ellos con capítulos específicos sobre comercio digital o digital trade provisions). Además, en 2024-2025 la UE ha firmado acuerdos de comercio digital "self-standing" con Singapur y con Corea del Sur-lo que se considera el primer y segundo acuerdo de este tipo-.

[13] Comisión Europea, "EU–US Data Privacy Framework: Questions and Answers on the Adequacy Decision," 13 de diciembre de 2022, https://ec.europa.eu/commission/presscorner/detail/de/qanda_22_7632

[14] Organización para la Cooperación y el Desarrollo Económicos (OCDE), "Declaration on Government Access to Personal Data Held by Private Sector Entities," OECD Legal Instruments, 13 de mayo de 2023, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

[15] Comité Europeo de Protección de Datos (EDPB), *Recomendaciones 02/2020 sobre las garantías esenciales europeas para medidas de vigilancia*, adoptadas el 10 de noviembre de 2020, https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_es

[16] A medida que consiguieran avanzar hacia una ley federal integral de privacidad y hacia un mayor compromiso con las transferencias de datos en entornos multilaterales, se verían inevitablemente empujados en esta dirección.

[17] El Acuerdo entre los EE. UU, México y Canadá (art. 19.11); y el Acuerdo de comercio digital entre los EE. UU. y Japón (art. 11) contienen amplias garantías sobre la capacidad de transferir datos a través de redes digitales transnacionales.

[18] EE. UU. recientemente ha protagonizado un cambio sustancial de postura en este ámbito lo que ha permitido que algunos estados asiáticos le tomen la delantera en materia de firma de acuerdos internacionales en este sentido.

de datos de carácter personal y de la privacidad. De forma reciente, esta cuestión se ha intentado incorporar sin éxito en las negociaciones comerciales multilaterales.

Asimismo los acuerdos de libre comercio de los EE. UU. y los de la UE[19] reconocen el derecho de los gobiernos a limitar las transferencias de datos si las consideran incompatibles con sus respectivas normativas internas, incluidas las de protección de la privacidad o las de seguridad nacional. Sin embargo, se observa que los acuerdos promovidos por EE. UU. poseen ventajas e insisten en que esas medidas reguladoras restrictivas sean las estrictamente necesarias[20]. Del mismo modo, los acuerdos estadounidenses hacen hincapié en que dichas medidas no constituyan una discriminación arbitraria o injustificable ni restricciones encubiertas al comercio de servicios entre Estados[21]. Para ello, este país incorpora referencias a las excepciones permitidas en virtud del Acuerdo General sobre el Comercio de Servicios (GATS)[22] de la Organización Mundial del Comercio (OMC). Por lo tanto, aunque la UE es parte del GATS y, sin perjuicio del compromiso de su cumplimiento, sus acuerdos comerciales bilaterales permiten expresamente a cada parte imponer las limitaciones que considere oportunas por razones de privacidad o protección de datos[23].

1.1. La Ruta 66 digital: la tecnología al servicio del mercado

La Ruta 66 es una conocida carretera federal creada en 1926 para cruzar los EE.UU. de costa a costa -con inicio en Chicago y final en California-, acercando la costa oeste a los emigrantes estadounidenses que soñaban con un futuro mejor. Aunque se concibió para ampliar las vías comerciales, terminó convirtiéndose en un símbolo de la libertad estadounidense. De tal modo, la Ruta 66 encarna el sueño americano y, por ello, adquiere una relevancia cultural significativa, al representar, entre otros aspectos, la nostalgia por una época de exploración y progreso.

De manera análoga a como la Ruta 66 simboliza esa sed de progreso y libertad, el enfoque estadounidense en materia de regulación de la economía digital se articula históricamente en torno a una fe inquebrantable en los mecanismos de mercado y a un escepticismo arraigado frente a la intervención gubernamental. Esta aproximación tecno-optimista -que hunde sus raíces en una cultura jurídica y política marcadamente liberal- se fundamenta en la convicción de que la innovación tecnológica se despliega con mayor eficacia allí donde el Estado limita su actividad regulatoria al mínimo indispensable. Desde esta perspectiva, la economía digital prospera principalmente gracias al dinamismo empresarial y a la autorregulación de las empresas tecnológicas, mientras que la intervención gubernamental se percibe como una carga que incrementa los costos y restringe el comportamiento innovador del sector privado.

Bajo esta visión tecno-libertaria, la regulación estatal no solo afecta negativamente la eficiencia de los mercados, sino que también podría socavar la libertad individual y la autonomía de empresas y ciudadanos. De este modo, la defensa de la innovación y del crecimiento económico opera como justificación económica para la no intervención, mientras que la protección de la autonomía personal y de la libertad individual funciona como argumento político orientado a minimizar el papel del Estado en la economía digital.

Estas convicciones se encuentran profundamente arraigadas en el régimen jurídico estadounidense. Ahora bien, el elemento normativo que mejor encarna este *ethos* regulatorio es la Sección 230 de

[19] Por el momento China presenta una posición expectante en materia de firma de acuerdos bilaterales y multilaterales en este ámbito, priorizando compromisos genéricos de *soft law* alineados con los principios que este Estado promueve.

[20] Aunque sus acuerdos no definen el criterio de necesidad, sí se hacen menciones concretas a "evitar carga regulatoria innecesaria en las transacciones electrónicas", – acorde con las restricciones permitidas en el art. XIV c) ii) y el art. XIV bis 1.b) del GATS – "asegurar que las restricciones a los flujos transfronterizos de información personal son necesarias y proporcionales a los riesgos presentados" o a que – acorde con las restricciones permitidas en el art. XIV a) y el art. XIV bis 1.b) del GATS – "ninguna parte prohibirá o restringirá la transferencia transfronteriza de información [...] cuando esta actividad sea para la realización de un negocio de una persona cubierta. Esto no impide que una parte adopte o mantenga una medida incompatible que sea necesaria para alcanzar un objetivo legítimo de política pública, siempre que la medida: (a) no se aplique de forma que constituya un medio de discriminación arbitraria o injustificable, o una restricción encubierta al comercio; y (b) no imponga restricciones a las transferencias de información mayores a las que se requieren para alcanzar el objetivo."

[21] Acuerdo de comercio entre los EE. UU., México y Canadá, art. 19.11.2. Una medida no cumpliría esta condición si concede un trato diferente a las transferencias de datos únicamente sobre la base de que son transfronterizas de una manera que modifica las condiciones de competencia en detrimento de los proveedores de servicios de otra parte.

[22] Organización Mundial del Comercio (OMC), *Acuerdo General sobre el Comercio de Servicios* (AGCS), 1994, arts. XIV y XIV bis, en https://www.wto.org/english/tratop_e/serv_e/gatsintr_e.htm Véase Acuerdo de libre comercio entre la UE y Nueva Zelanda, arts. 12.5 y 25.1.2.

[23] Véase Acuerdo de libre comercio entre la UE y Nueva Zelanda, arts. 12.5 y 25.1.2.

la Communications Decency Act (CDA) de 1996, una disposición que se ha caracterizado como la "piedra angular de internet" en los EE.UU.[24] La norma otorga amplia inmunidad a los intermediarios en línea frente a responsabilidades derivadas de contenidos generados por terceros.

A la luz de este escenario, y como se ha indicado, el planteamiento de la protección de los datos personales -si bien con un enfoque eminentemente sectorial- está profundamente arraigado en su historia al entender esa privacidad como la protección de la libertad, tal y como la concebía su Bill of Rights. De hecho, en los EE. UU., los agentes privados (responsables y encargados de tratamiento de datos) suelen estar protegidos frente a restricciones en su actividad por la Primera Enmienda. Por lo tanto, las entidades que tratan los datos estarían protegidas frente a posibles exigencias de los interesados o consumidores en relación con el tratamiento de sus datos. Además, en este país, las políticas en torno a la libertad en Internet han buscado continuamente "preservar y ampliar Internet como un espacio abierto y global para la libre expresión, para la organización y la interacción y para el comercio", tal y como confirmó la estrategia de la Casa Blanca sobre inteligencia artificial (IA)[25] bajo la presidencia de Joe Biden, y más recientemente la iniciativa del presidente Donald Trump para prevenir la fragmentación normativa entre Estados en materia de IA.

Mientras que, en virtud de la Primera Enmienda, la libertad de expresión goza de una sólida protección en los EE. UU., la protección de datos se regula de manera fragmentada a través de algunas leyes federales sobre privacidad y de un amplio conjunto de leyes estatales. Estas normas o bien se limitan al sector público, o bien son específicas del tipo de información o del medio a través del cual se difunde (por ejemplo, la información sanitaria, la privacidad de los vídeos o las comunicaciones electrónicas). En este sentido, no existen restricciones generales a la transferencia de datos personales por parte de entidades privadas, y la autorregulación, junto con las denominadas "mejores prácticas", constituye el modelo predominante de protección de la privacidad.

En lo relativo a la protección de los ciudadanos, el legislador estadounidense se centra en las restricciones que permite la Cuarta Enmienda de la Constitución en lo que respecta a la recopilación y al uso de datos personales por parte del gobierno, y no de los actores privados. Este último constituye el enfoque de la normativa europea en términos generales, la cual se encuentra más orientada al cumplimiento normativo (*compliance*). Esta diferencia se ilustra en la ambigüedad existente en EE. UU. respecto de la definición de los roles de responsable y encargado del tratamiento de los datos (agentes privados), frente a la claridad en su definición y alcance en el RGPD[26].

En esta situación normativa, no existe siquiera una definición uniforme y coherente del concepto de datos de carácter personal, tampoco sobre los datos sensibles, más conocidos en Europa, donde están claramente definidos como "categorías especiales de datos personales". Adicionalmente, los datos se consideran un bien susceptible de transacción y, en consecuencia, su exportación no está limitada en absoluto. Por lo general, existe una tendencia hacia una gobernanza liberal, basada en los intereses del mercado, en contraste con la gobernanza socialmente protectora y cimentada en los derechos de los interesados que existe en la UE.

En contraste, los EE. UU. conciben las normas que prohíben la transferencia internacional de datos como limitaciones a la libertad de circulación de la información, que ahoga la competencia y perjudica a las empresas digitales[27]. A pesar de ello, se observa que, desde el final de la Segunda Guerra Mundial, este país atiende de manera fundamental la lógica de la seguridad nacional, el orden público y la soberanía. Empero, en la última década se ha observado un replanteamiento de la cuestión que no parece derivar en un cambio de paradigma rápido y fácil. Esto es especialmente evidente a partir de las reacciones a la sentencia del Tribunal de Justicia de la UE (TJUE) en el asunto Schrems II[28] que, por lo demás, muestran significativas diferencias en los niveles de regulación federal y estatal.

[24] *Communications Decency Act*, 47 U.S.C. § 230 (1996).

[25] Accesible en: The White House, "Fact Sheet: Biden-Harris Administration Announces New AI Actions and Receives Additional Major Voluntary Commitments on AI," 26 de julio de 2024. https://www.whitehouse.gov/briefing-room/statements-releases/2024/07/26/fact-sheet-biden-harris-administration-announces-new-ai-actions-and-receives-additional-major-voluntary-commitment-on-ai/. Visitado el 20 de diciembre de 2025.

[26] David Carrizo, "Reflexiones a propósito de la protección de datos en el escenario global digital: El derecho de daños en la litigiosidad internacional," *Revista Boliviana de Derecho*, no. 31 (2021): 451, destacando que estos conceptos son funcionales (tienen por objeto asignar responsabilidades en función del papel real de cada parte en el tratamiento de los datos) y autónomos (deben interpretarse conforme al derecho de la UE).

[27] Otero García-Castrillón. "Protección…", 47.

[28] Tribunal de Justicia de la Unión Europea, asunto C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd y Maximillian Schrems*, sentencia de 16 de julio de 2020 (Schrems II).

Asimismo, algunos estados, como California, Colorado, Connecticut y Virginia cuentan formalmente con idénticos derechos a los garantizados por el RGPD, lo que alcanza un grado de protección de datos de carácter personal similar al europeo. Con todo, la regulación federal es fragmentaria; es decir, el marco regulador está orientado al comercio, por lo que no tiene un principio de prohibición y las escasas normas que existen sobre protección de datos personales son sectoriales y no exhaustivas. En la actualidad, se plantea la adopción de una normativa general a nivel federal que incluya los mismos siete principios y los seis derechos de los interesados que se contemplan en el RGPD. En todo caso, se advierte que el derecho a restringir el tratamiento de datos personales y el derecho a no ser objeto de la toma de decisiones automatizadas y de elaboración de perfiles solo se incluirá parcialmente.

Como es sabido, fue el caso Microsoft contra la Oficina Federal de Investigaciones (FBI por sus siglas en inglés) el que detonó el cambio de la Clarifying Lawful Overseas Use of Data Act (CLOUD Act)[29] para darle carácter extraterritorial. Ahora bien, este cambio fue posible dado que la CLOUD Act se modificó para permitir a las fuerzas de seguridad solicitar directamente (y obtener) datos tratados por proveedores de servicios con sede en el extranjero[30]. En tal sentido, esto ha derivado en el actual panorama de decisiones de adecuación (más conocidos como escudos de privacidad) débiles que se han ido implementando y también invalidando en hasta tres ocasiones desde 2015 hasta la fecha, con la notable supervivencia de su última versión a su paso por el TJUE en septiembre de 2025.

En el caso de referencia, Microsoft se negó a facilitar al FBI la información almacenada en sus servidores de Irlanda. Aunque Microsoft consiguió evitar el acceso a la información, el gobierno de los EE. UU. actuó rápido para cambiar la redacción del CLOUD Act y evitar que ese caso pudiera replicarse en el futuro. El objetivo estadounidense era claro: garantizar el acceso ilimitado por parte de las autoridades estadounidenses a la información almacenada por empresas norteamericanas en el extranjero. Hasta la fecha, esta es la única normativa estadounidense no estrictamente sectorial con carácter extraterritorial. En ese sentido, el derecho estadounidense lleva una década sorteando internamente un conflicto de intereses indudablemente grave en la legislación sobre privacidad. Este conflicto consiste en la confrontación entre la antigua lógica de la seguridad nacional, el orden público y la soberanía en torno a las que se desarrolló el discurso de la privacidad desde el final de la Segunda Guerra Mundial, frente al replanteamiento de la última década. En efecto, esta última visión está más enfocada hacia la explotación extensiva de las oportunidades económicas basadas en la economía del dato.

Algunas leyes estatales en la materia, como las de California, Colorado, Connecticut y Virginia que se han referido, persiguen una aplicación extraterritorial similar a la prevista a nivel federal en el CLOUD Act. No obstante, en estos cuatro Estados los mecanismos de transferencia desarrollados presentan un ámbito de aplicación acotado a nivel sectorial. Esta limitación viene definida por las propias normas estatales, las cuales son de aplicación exclusiva a determinados sectores de actividad, como el sanitario, el financiero o el educativo, entre otros. Dicha restricción sectorial imposibilita su aplicación transversal.

Una aplicación transversal permitiría maximizar el valor añadido de estos mecanismos en la economía digital, especialmente si se considera que las fronteras que delimitan unos sectores de otros son cada vez más difusas, lo que genera una demanda creciente de transversalidad para evitar que tales instrumentos resulten obsoletos. Un ejemplo de ello es la creciente incursión de los proveedores tradicionales de servicios tecnológicos en sectores regulados, como el financiero. Cuando un mecanismo de transferencia solo es aplicable de forma estricta a un sector determinado, cualquier iniciativa de negocio que implique una incursión comercial transectorial podría quedar fuera de su ámbito de aplicación. Esta situación generaría una desventaja competitiva para el libre flujo de información que los competidores más innovadores buscan desarrollar.[31] Se trata de una problemática inherente a la economía del dato y de un debate ya clásica en el seno de la OMC sobre la clasificación de productos y servicios digitales mixtos dentro del ámbito de aplicación del GATT o del GATS.

Asimismo, las mencionadas leyes estatales incorporan algunos requisitos puntuales de almacenamiento local o *data localisation*. De tal modo, este tipo de exigencias, habituales en los

[29] Accesible en: *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act), S.2383, 115th Cong. (2018). Visitado el 27 de diciembre de 2025.

[30] En teoría la actual redacción de la *CLOUD Act* simplemente elimina los conflictos de leyes y no afecta a la jurisdicción sobre los proveedores extranjeros. Éstos están estrictamente limitados por el requisito de jurisdicción personal contenido en la Cláusula de *Due Process* de la Quinta Enmienda de la Constitución.

[31] Los productos de seguros comercializados por Amazon Marketplace son un buen ejemplo de esta situación pues su clasificación dentro de la normativa aseguradora los lastra.

sistemas asiáticos, implican restricciones totales o parciales a la transferencia internacional de datos y derivan de posturas proteccionistas en materia de privacidad.

Un aspecto positivo de estas leyes estatales, en comparación con la perspectiva europea, es la adopción de un enfoque de rendición de cuentas a posteriori o *light touch*, alineado con las recomendaciones de la OCDE. Así, dichas recomendaciones se centran en esquemas de colaboración con la industria y entre reguladores, así como en la corregulación y la autorregulación mediante códigos de conducta, con el fin de facilitar la interacción entre proveedores y usuarios.

Este planteamiento contrasta con las normativas europeas en la materia, que optan por enfoques de responsabilidad proactiva en la rendición de cuentas. En este sentido, el enfoque europeo aún presenta un amplio margen de desarrollo en materia de colaboración con la industria y autorregulación. Si bien el RGPD contempla cierta regulación sobre códigos de conducta, especialmente en relación con las transferencias internacionales de datos, se trata de un ámbito que, hasta el momento, apenas se ha desarrollado.

En septiembre de 2021, el Servicio de investigación del Congreso de EE. UU. publicó un informe sobre las opciones para facilitar la vuelta a la normalidad de las transferencias internacionales entre los EE.UU. y la UE. El informe en cuestión mencionaba expresamente, entre otras alternativas, la creación de una Ley Federal de Privacidad. Sin embargo, esta iniciativa ha quedado estancada. El motivo es evidente: la cuestión parecía haberse resuelto con la Transatlantic Data Privacy Framework[32], al menos a nivel político y temporalmente. Una posible Ley Federal de Privacidad era un gran argumento de negociación con la UE. En consecuencia, una legislación federal habría facilitado la uniformidad normativa entre los diferentes Estados de Norteamérica. Ahora bien, esto no solamente habría atajado la problemática de la fragmentación. Asimismo, habría facilitado que la UE pudiera llevar a cabo un reconocimiento de adecuación *standard* de los EE. UU., en lugar de continuar con el sistema de escudos de privacidad.

Sin embargo, con el reconocimiento del Transatlantic Data Privacy Framework y su reciente resistencia a la embestida del activista Max Schrems en la UE, los EE. UU. han ganado tiempo y pueden permitirse despriorizar la elaboración de dicha norma, al considerar que su principal motivación para plantearla había sido solventar el desencuentro con la UE tras la caída del Privacy Shield. No obstante, el activista Max Schrems ha recurrido a la Sentencia desfavorable a sus pretensiones de septiembre de 2025 sobre la validez de este instrumento ante el TJUE, por lo que se espera un futuro pronunciamiento al respecto a partir de 2026[33], que promete revolucionar de nuevo el panorama transatlántico, e impulsar a EE. UU. a retomar la idea de una Ley Federal de Privacidad.

A la luz de este escenario, el futuro de la regulación de la privacidad y la protección de datos en los EE. UU no parece estar claro. Si bien, cabe intuir, a tenor de las propuestas legislativas -Protecting Americans' Data from Foreign Adversaries Act[34] y la Executive Order 14117-, que ese porvenir promete la incursión de EE. UU en el terreno de las barreras al comercio basadas en motivos de seguridad nacional. Por lo tanto, un cambio de paradigma trascendería las medidas de vigilancia existentes que han sido detonantes del vaivén transatlántico, es decir, un estado cíclico de *fragile trust*.

En esta línea de frágil confianza, en 2021, se halló que un estudio realizado a petición del Comité de Libertades Civiles del Parlamento Europeo destacaba la escasa probabilidad de que las normativas de privacidad estatales, ni la federal lleguen a ofrecer una protección esencialmente equivalente a

[32] Accesible en: "Marco de privacidad de datos UE-EE. UU.", Data Framework Program [DFP] https://www.dataprivacyframework.gov/EU-US-Framework. Visitado el 20 de diciembre de 2025.

[33] Con ocasión de la publicación del *Transatlantic Privacy Framework*, el activista Max Schrems, responsable de llevar ante el TJUE los dos Escudos de privacidad anteriores, ya manifestó que desde su ONG Noyb "*Tenemos varias opciones de impugnación ya en el cajón, aunque estamos hartos de este ping-pong jurídico. Actualmente esperamos que esto vuelva al Tribunal de Justicia a principios del año que viene." A la espera de esta decisión, el TJUE resolvió en septiembre de 2025 el caso T-553/23, Latombe contra Comisión. Aunque se trata de un caso de alcance más limitado, el Tribunal de Justicia no suspendió el nuevo acuerdo considerando que las pequeñas mejoras de la Comisión han sido suficientes. No obstante, Schrems ha declarado no descartar que el TJUE resuelva en otro sentido en un caso de mayor alcance. Al fin y al cabo, durante los últimos 23 años, todos los acuerdos entre la UE y EE. UU. han sido declarados inválidos con carácter retroactivo, haciendo ilegales todas las transferencias de datos realizadas por las empresas en el pasado; parece que ahora vamos a añadir otros dos años de este ping-pong*". *En*: NOYB – European Center for Digital Rights, "La Comisión Europea da un tercer asalto ante el TJUE a las transferencias de datos entre la UE y EE. UU.," 10 de agosto de 2023, en https://noyb.eu/es/european-commission-gives-eu-us-data-transfers-third-round-cjeu. Visitado el 23 de diciembre de 2025.

[34] Este proyecto de ley incluiría los mismos siete principios que el RGPD a nivel federal y seis derechos de los interesados reconocidos en el RGPD, aunque el derecho de limitación de datos de carácter personal y el derecho a no ser objeto de decisiones automatizadas y a la elaboración de perfiles sólo se incluirían parcialmente.

la del RGPD a medio plazo[35], independientemente del acercamiento temporal de posturas derivado de la Transatlantic Data Privacy Framework[36].

1.2. El Camino de Santiago digital: la tecnología al servicio del ser humano

El Camino de Santiago constituye una red histórica de rutas de peregrinación cristianas que convergen en la Catedral de Santiago de Compostela, donde se consideran enterrados los restos del apóstol Santiago, y que ha atraído a peregrinos desde la Edad Media por motivos religiosos, culturales y personales.

No se trata de una única ruta, sino de un entramado de senderos que atraviesa diversos países de la Europa continental. En tanto red de itinerarios recorridos por las motivaciones referidas, el Camino de Santiago puede entenderse como una representación de una UE legislativamente fragmentada[37] y orientada por un compromiso ideológico con una economía digital centrada en el ser humano, con marcados componentes culturales.

En términos estrictamente regulatorios, la normativa europea ha sido la más influyente a nivel global y ha moldeado legislación de todas las regiones del mundo en mayor o menor medida. El término "efecto Bruselas[38]" se acuñó en referencia a este fenómeno.

La UE reconoce que los productos y servicios innovadores desarrollados por las grandes empresas tecnológicas generan beneficios sustanciales para las personas y las sociedades, motivo por el cual considera deseable promover su desarrollo. Esta valoración positiva convive con profundas preocupaciones en torno a la deriva estructural de la economía digital, caracterizada por una creciente concentración de poder económico y político en un número reducido de plataformas globales. Desde la perspectiva de la UE, una economía excesivamente concentrada facilita que determinadas empresas abusen de su posición dominante, restrinjan la competencia y perjudiquen tanto a competidores como a consumidores.

A partir de estas preocupaciones, la UE ha impulsado una intensa agenda regulatoria durante la última década. Como resultado, este proceso ha dado lugar a un entramado normativo que penaliza determinados modelos de negocio de las grandes empresas tecnológicas y refuerza las salvaguardias de los derechos fundamentales en el entorno digital.

Por otro lado, la protección de datos de carácter personal se proclamó como derecho fundamental en la Carta de los Derechos Fundamentales de la UE[39] (CDFUE, art. 8); asimismo, se consideró parte del contenido del derecho a la vida privada y familiar en el Convenio Europeo de Derechos Humanos y Libertades Fundamentales (CEDH, art. 8) sobre el que existe una abundante jurisprudencia del Tribunal Europeo de Derechos Humanos[40] (TEDH)[41].

Si bien la confianza y certeza jurídica en el tratamiento de datos se encuentran en la base reguladora de todo el entorno europeo, la adopción de un reglamento (el RGPD) resultaba fundamental. Por consiguiente, al establecer un cuerpo normativo común en todos los países de la UE, se permite la igualdad de condiciones necesarias para un mercado único digital[42]. En este sentido, la UE reconoce

[35] Parlamento Europeo, *Exchanges of Personal Data after the Schrems II Judgment* (Bruselas: Parlamento Europeo, 2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pd. Visitado el 20 de diciembre de 2025.

[36] U.S. Department of Commerce, "EU–U.S. Data Privacy Framework."

[37] Debido a su mercado único inconcluso.

[38] Concepto entendido como la capacidad unilateral de la UE para regular los mercados mundiales de forma no coercitiva, es decir, apoyándose únicamente de su capacidad de presión comercial. Eso se materializa estableciendo normas en diferentes materias como competencia, protección del medio ambiente o seguridad alimentaria. Estándares que sus colaboradores comerciales buscan voluntariamente incorporar en la medida de lo posible a sus legislaciones para garantizar la continuidad de las relaciones comerciales con la UE.

[39] Así como en algunas constituciones nacionales, como en el caso de la española (art. 18).

[40] La doctrina del TEDH ha establecido que el respeto a la vida privada y familiar resulta infringido cuando se accede o se utilizan datos de un individuo sin su consentimiento, salvo si este uso está amparado por la ley y, además, resulta necesario y proporcional al objetivo perseguido, y se ha garantizado al interesado la oportunidad de obtener revisión judicial de la actuación.

[41] Otero García-Castrillón. "Protección…", 38.

[42] Carrizo, "Reflexiones…", 462.

la dimensión económica del dato, por lo que el TJUE interpreta los mecanismos previstos para velar por el mantenimiento del estándar comunitario en las exportaciones de datos[43] y, en consecuencia, aborda su aplicación extraterritorial.

En el asunto *Salemink*[44], el abogado general afirmó que "a efectos de la UE, el territorio de los Estados miembros es el área (no necesariamente territorial, en el sentido espacial o geográfico) de ejercicio de las competencias de la Unión", lo que calificó la conexión entre el ejercicio de la soberanía y un territorio físico más próxima de una verdad contingente que necesaria[45]. Tras la Sentencia *Schrems I*[46], el supervisor europeo de protección de datos indicó que la normativa europea sobre transferencias internacionales de datos de carácter personal se basa en "un grado razonable de pragmatismo con el fin de permitir la interacción con otras partes del mundo". No obstante, se evidencia que algunos autores consideran que esta regulación no busca un equilibrio razonable entre los estándares propios y los de terceros países, sino la afirmación unilateral de los valores de la UE. Por tal motivo, es poco realista esperar soluciones internacionales sin que los demás Estados estén dispuestos a efectuar concesiones[47].

De hecho, numerosos países europeos, entre ellos España, no implementaron normas de privacidad hasta la etapa de negociación de la Directiva europea de protección de datos (DPD) en 1995. A partir de la DPD es cuando la protección de datos se convirtió en un requerimiento esencial para acceder al comercio interior que ofrece la UE. Otro ejemplo llamativo consiste en el caso de Polonia, que en 1997 (siete años antes de convertirse en Estado miembro) ya declaraba en su norma nacional de privacidad que se sometía a la DPD. En consecuencia, resulta evidente que el acceso a la UE requería conciliar con el *acquis* que, entre otros, incluía la normativa de privacidad. Igualmente, los propios reportes sobre el acceso a la UE demuestran un cambio a lo largo del tiempo en la visión de la UE sobre el rol de la protección de datos en la integración europea. Al respecto, se observa que originalmente el capítulo en el que se incorporaban las cuestiones de privacidad solía ser el de "Freedom to provide services". En consonancia con las últimas adhesiones, como la de Croacia, se evidencia un cambio de paradigma con su incorporación en la sección de derechos fundamentales[48].

En ese orden de ideas, plantear la norma de privacidad a todos los territorios de la UE ha sido un aspecto crítico del proyecto original de la creación del Mercado Digital Único. Ahora bien, la adopción de normativas de privacidad no ha sido el único objetivo europeo, sino también asegurar que las existentes en cada uno de los países que se han adherido cumplan con los estándares europeos.

Fuera de su territorio, la UE también ha utilizado su poder negociador en los acuerdos de libre comercio para persuadir a sus *partners* comerciales hacia su propia visión de la privacidad. Por consiguiente, es notable la progresiva incorporación en las negociaciones y acuerdos de libre comercio con países terceros, de referencias e incluso provisiones completas en materia de privacidad y protección de datos. Un buen ejemplo es el art. 30 del acuerdo de libre comercio entre la UE y Chile[49], que se encuadra dentro del bloque de cooperación económica y que se refiere a este aspecto de la privacidad como "facilitador del comercio".

En efecto, las decisiones de adecuación de la Comisión Europea cumplen un rol fundamental en la propagación de la perspectiva de la UE sobre la privacidad. Aunque las decisiones de adecuación funcionan en paralelo a los acuerdos comerciales entre las partes, dependen de estos acuerdos comerciales. Además, se presenta la particularidad de que las decisiones de adecuación se

[43] Otero García-Castrillón. "Protección…", 41.

[44] Conclusiones del Abogado General Pedro Cruz Villalón, presentadas el 8 de septiembre de 2011, asunto C-347/10, *A. Salemink v Raad van bestuur van het Uitvoeringsinstituut Werknemersverzekeringen*, ECLI:EU:C:2011:562, párrs. 54–57.

[45] Taylor Mistale, "Limits That Public International Law Poses on the European Union Safeguarding the Fundamental Right to Data Protection Extraterritorially," en T*ransatlantic Jurisdictional Conflicts in Data Protection Law: Fundamental Rights, Privacy and Extraterritoriality*, ed. Taylor Mistale (Cambridge: Cambridge University Press, 2023), 70.

[46] Tribunal de Justicia de la Unión Europea, asunto C-362/14, *Maximillian Schrems v Data Protection Commissioner*, sentencia de 6 de octubre de 2015 (*Schrems I*).

[47] Christopher Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems", *German Law Journal*, 18, n°. 4 (2017): 917.

[48] Diario Oficial de la Unión Europea (DOUE), L 112, 24 de abril de 2012. Visitado el 27 de diciembre de 2025.

[49] Unión Europea y República de Chile, *Agreement Establishing an Association between the European Community and Its Member States, of the One Part, and the Republic of Chile, of the Other Part*, 2002, https://eur-lex.europa.eu/resource.html?uri=cellar:f83a503c-fa20-4b3a-9535-f1074175eaf0.0004.02/doc_2&format=pdf. Visitado el 28 de diciembre de 2025.

reconocen generalmente de forma unilateral por parte de la UE tras la formalización de dichos acuerdos. De esta forma, se evidencia que, al negociar un acuerdo comercial con la UE, la contraparte solo tiene la capacidad de influir en los términos del propio acuerdo comercial en cuestión. De tal modo, la UE[50] siempre mantendrá la discrecionalidad y unilateralidad con respecto a la decisión de adecuación. Un ejemplo de lo anterior radica en el acuerdo de libre comercio entre la UE y el Reino Unido, donde no se estableció ninguna limitación temporal relevante. Ahora bien, se expuso que la decisión de adecuación que la UE reconoció posteriormente al Reino Unido incluía una limitación temporal de cuatro años. En consecuencia, independientemente de los términos del acuerdo comercial, se retenía esa capacidad unilateral de no renovar la decisión de adecuación en cuestión en 2025. En cualquier caso, la renovación ha tenido lugar satisfactoriamente por un periodo de seis años más.

A la luz de este contexto, queda patente que el efecto Bruselas está totalmente vigente en materia de privacidad, no solo por la extraterritorialidad del RGPD. De hecho, la privacidad y la protección de datos son probablemente de los ejemplos más prominentes de dicho efecto.

Sin embargo, para mantener su posición negociadora privilegiada, la UE aún tiene pendiente la tarea de equilibrar los conceptos de protección de datos y de proteccionismo de los datos, una dicotomía que sus acuerdos de libre comercio buscan abordar fundamentalmente mediante la incorporación de prohibiciones a la localización de datos, la facilitación de los flujos internacionales y la asunción de compromisos concretos, como los relativos a la minimización de datos. En cualquier caso, el acercamiento normativo resulta complejo, pues solo podría alcanzarse de manera parcial.

Incluso en aquellos casos aislados en los que dicho acercamiento fuera total desde un punto de vista formal -como ha ocurrido con la normativa de protección de datos de Andorra o en el caso de Brasil, que acaba de obtener el reconocimiento referido tras una década de espera-, ello no implica necesariamente una implementación idéntica. La mera adopción de una legislación prácticamente equivalente al RGPD no garantiza una interpretación consistente en la práctica, dadas las diferencias culturales respecto de la UE. De hecho, en la propia UE persisten múltiples divergencias entre los estándares de aplicación de las normativas nacionales y el RGPD, pese al alto grado de integración que este último pretendía alcanzar y sin perjuicio de su jerarquía normativa superior[51]. En efecto, Estados como Alemania -con su particular cruzada por el *cloud* nacional para el sector educativo- evidencian una tendencia al localismo que perjudica significativamente la consolidación del proyecto de Mercado Digital Único europeo.

La UE tiene en el contexto del Digital Ómnibus la oportunidad de reafirmar su objetivo que no es otro que garantizar que los estándares regulatorios europeos se conviertan en estándares de alcance global. Esto es, estándares que no sean meramente seguidos en el plano internacional, sino universalmente respetados, en la medida en que están dotados de la credibilidad que únicamente puede proporcionar un pragmatismo responsable.

1.3. La ruta de la seda digital: la tecnología al servicio del Estado

La Ruta de la Seda constituye uno de los pilares históricos más influyentes en la conformación de la identidad comercial y geopolítica de China. Desde la Antigüedad, este conjunto de rutas terrestres y marítimas articula un espacio de intercambio económico, tecnológico y cultural que permite a China proyectar su influencia a lo largo de Asia, Oriente Próximo, África y Europa. En la actualidad, la evolución del ecosistema digital chino y, en particular, la concepción jurídica del comercio digital y del tratamiento de los datos personales muestran una continuidad estructural con este legado histórico: China concibe el flujo de información como un recurso estratégico para asegurar la estabilidad interna, el desarrollo económico y la proyección internacional. En consecuencia, se debe explorar la comparativa entre ambos fenómenos —la Ruta de la Seda y el régimen chino del comercio digital— con el fin de identificar los elementos históricos, jurídicos y culturales que configuran la particular visión china sobre los servicios digitales basados en datos.

La Ruta de la Seda no constituye únicamente un corredor comercial, sino también un sistema de gobernanza. La Corte imperial establece estrictos mecanismos de control sobre las mercancías, la diplomacia y la movilidad, con el objetivo de garantizar la seguridad de las fronteras y regular

[50] Esta unilateralidad no solamente correspondería a la UE, sino a cualquier otro Estado que incorpore los mecanismos de decisiones de adecuación a su legislación. Con todo, en la actualidad ningún Estado ha optado por esta vía tras un reconocimiento de adecuación de la UE. En su lugar, la práctica es replicar ese reconocimiento por parte del Estado en cuestión para beneficiarse del intercambio comercial con la UE.

[51] Merece la pena destacar las constantes tensiones entre normas nacionales y autoridades de protección de datos europeas en cuestiones como la regulación del consentimiento para cookies, en materia de legitimación del tratamiento de datos biométricos o de la monitorización en el ámbito laboral.

la entrada y salida de conocimientos tecnológicos considerados estratégicos. Esta tradición de control estatal sobre los flujos comerciales y transacciones resulta clave para comprender la aproximación contemporánea de China al derecho del entorno digital. En contraste con los modelos liberalizantes de los EE.UU. o los enfoques garantistas de la UE, China adopta un esquema centralizado y normativamente robusto, en el que el Estado asume un papel preponderante en la regulación del comercio digital y en la gobernanza de los datos personales.

En el contexto actual, China estructura un marco jurídico orientado a reforzar su soberanía digital, en el que destacan la *Cybersecurity Law* (2017), la *Data Security Law* (2021) y la *Personal Information Protection Law* (PIPL, 2021). Aunque esta última presenta paralelismos formales con el RGPD de la UE, su lógica subyacente difiere sustancialmente: mientras que en Europa el foco se sitúa en la protección del individuo frente a los poderes públicos y privados, en China el énfasis recae en la protección del Estado y en la preservación del orden social. La información personal se concibe, de manera simultánea, como un recurso económico y como un activo estratégico cuya circulación debe alinearse con los objetivos nacionales de la misma forma que lo hacía el comercio de mercancías que transitaba por la Ruta de la Seda.

El paralelismo con la Ruta de la Seda resulta evidente, dado que, del mismo modo que en la Antigüedad el Imperio chino regulaba los intercambios para asegurar la estabilidad interna y la proyección internacional, en la actualidad China controla los flujos de datos con el fin de evitar riesgos geopolíticos, fomentar la innovación autónoma y garantizar la seguridad nacional. En el marco digital contemporáneo, la información se convierte en la nueva mercancía estratégica. Así como la seda y la pólvora desempeñan un papel central en el comercio imperial, los datos adquieren hoy una función clave en la competitividad de las empresas chinas y en la expansión global de sus plataformas digitales.

Asimismo, la Ruta de la Seda genera asimetrías de poder, en la medida en que China garantiza el acceso al comercio a aquellos territorios que aceptan sus normas y estructuras diplomáticas. En la esfera digital contemporánea se observa una dinámica similar: mediante la Iniciativa de la Franja y la Ruta Digital (*Digital Silk Road*), China exporta infraestructuras tecnológicas, estándares de conectividad y modelos de gobernanza digital que refuerzan su influencia global en ámbitos como las telecomunicaciones, la inteligencia artificial y la gestión de plataformas. En efecto, este proceso reproduce la lógica histórica de creación de espacios interdependientes bajo liderazgo chino.

No obstante, existen diferencias significativas entre ambos contextos. Mientras que la Ruta de la Seda ofrece un espacio de intercambio relativamente abierto, aunque sometido a supervisión imperial, el modelo digital chino contemporáneo prioriza la seguridad nacional por encima de la libertad individual o de la libre circulación de la información. La visión china del comercio digital se inscribe en una concepción más amplia de la "soberanía digital", en la que el control de las plataformas, la infraestructura y los datos resulta esencial para preservar la estabilidad política y la autosuficiencia tecnológica. Esta orientación contrasta con la dinámica transnacional y descentralizada del comercio que caracteriza, en gran medida, a la Ruta de la Seda tradicional.

El modelo regulatorio digital de China se fundamenta, en consecuencia, en un principio estructural: la primacía del control político del Estado y del Partido Comunista de China (PCCh) en la gobernanza del entorno digital. Desde principios del siglo XXI y, de manera más acentuada, bajo la presidencia de Xi Jinping, la estrategia digital china deja de concebir la tecnología como un espacio de autonomía social y pasa a integrarla explícitamente como un instrumento de cohesión política, estabilidad social y legitimidad estatal. Esta orientación se encuentra ampliamente documentada tanto en fuentes oficiales del gobierno chino como en la literatura académica comparada sobre autoritarismo digital[52].

Simultáneamente, China ha demostrado que un modelo de regulación fuertemente estatal y centralizado puede coexistir con una industria tecnológica dinámica, innovadora y de alcance global. Empresas como Alibaba, Tencent, ByteDance, Huawei o Xiaomi se han convertido en actores fundamentales para el crecimiento económico del país y para su ascenso geopolítico, situación que ha reforzado ante la ciudadanía la legitimidad del modelo de desarrollo liderado por el PCCh[53].

En este contexto, el modelo chino se configura como un contrapunto normativo frente a los enfoques occidentales dominantes previamente referidos: el modelo estadounidense orientado al mercado y el europeo centrado en la protección de derechos fundamentales. De tal modo, China

[52] Rogier Creemers, "China's Conception of Cyber Sovereignty: Rhetoric and Realization," en *Governing Cyberspace: Behavior, Power, and Diplomacy*, eds. Dennis Broeders y Bibi van den Berg (Lanham, MD: Rowman & Littlefield, 2020); Rebecca MacKinnon, *Consent of the Networked*: The Worldwide Struggle for Internet Freedom (New York: Basic Books, 2012).

[53] Adam Segal, *When China Rules the Web: Technology in Service of the State* (New York: Council on Foreign Relations, 2018); Gérard Roland y Nancy Qian, "The Evolution of China's Development Strategy," NBER Working Paper no. 29343 (Cambridge, MA: National Bureau of Economic Research, 2021), https://doi.org/10.3386/w29343

posee una larga tradición de restricción informativa y control de las comunicaciones. Desde la era imperial, las élites gobernantes temieron que la circulación sin control de ideas políticas pudiera generar contestación, un patrón que ha persistido en las distintas etapas del gobierno chino[54]. Tras la disponibilidad de acceso público a internet en 1995, el gobierno instauró el conocido "Gran Cortafuegos" (*Great Firewall*), una infraestructura técnico-regulatoria que combina filtrado, bloqueo de sitios *web* y mecanismos administrativos de censura.

Informes institucionales como los del Freedom House de 2022 y estudios académicos documentan cómo esta estructura limita el acceso a periódicos en línea y redes sociales[55]. En consecuencia, los ciudadanos solo pueden acceder mediante redes privadas virtuales (VPN por sus siglas en inglés), cuya utilización también está sujeta a regulaciones estrictas del Estado. Desde 2013, con la llegada de Xi Jinping al gobierno, el enfoque gubernamental hacia el ecosistema digital se ha radicalizado. Xi Jinping ha afirmado repetidamente que internet puede contener "energía negativa" capaz de socavar la "estabilidad social", razón por la cual el Estado debe "purificar" el espacio digital.

Bajo este marco conceptual, el gobierno ha aprobado tres leyes clave que institucionalizan el autoritarismo digital: a) la Ley de Seguridad Nacional de 2015, que reafirma la potestad del Estado para prevenir y sancionar cualquier actividad que amenace la unidad nacional, la soberanía o la estabilidad política; b) la Ley de Ciberseguridad previamente referida, que obliga a individuos y organizaciones a utilizar Internet, pero desde el respeto por el orden público y las "normas morales socialistas", además, establece los requisitos de localización de datos y controles sobre la infraestructura crítica; y c) la Ley de Seguridad de los Datos previamente referida, que restringe la transferencia internacional de datos y confiere al Estado autoridad para acceder y procesar información en nombre de la seguridad nacional. En consecuencia, estas normas[56] consolidan un marco en el que la tecnología queda jurídicamente subordinada al Estado.

En el plano comercial, la entrada de China en la OMC en 2001 propulsó sus relaciones comerciales con la UE y EEUU. China es parte del Regional Comprehensive Economic Partnership Agreement (RCEP), que contiene un capítulo específico sobre comercio electrónico con disposiciones relevantes sobre protección de la información personal, transferencias transfronterizas y localización de datos. También cuenta con acuerdos de libre comercio (TLC) bilaterales con disposiciones o capítulos de comercio electrónico con referencias a privacidad o protección de datos. En general, China tiene una red extensa de TLC bilaterales (por ejemplo, con Australia, Nueva Zelanda, Suiza, Islandia, Pakistán, Chile, Perú, Costa Rica, Georgia, Mauricio, Camboya, y acuerdos de alcance especial con Hong Kong y Macao, entre otros). En muchos de ellos, especialmente los más recientes o actualizados, aparecen capítulos de comercio electrónico, pero no todos incluyen reglas explícitas sobre flujos transfronterizos de datos, limitaciones de localización o un estándar detallado de privacidad comparable a otros modelos destacados en la región. Entre aquellos que sí incorporan reglas explícitas en este sentido destaca el TCL entre China y Corea del Sur. Este TLC incorpora un capítulo de comercio electrónico que contempla, de forma expresa, la protección de la información personal en el entorno del comercio electrónico en términos de cooperación o estímulo normativo. Hoy el comercio digital entre la UE y China continua al alza, pero está crecientemente condicionado por cuestiones regulatorias, geopolíticas y de soberanía tecnológica.

Retomando la cuestión sobre la subordinación tecnológica al Estado, la literatura contemporánea sobre autoritarismos digitales destaca que China no aplica una censura absoluta, sino una censura calibrada (*optimal censorship*) que permite cierto margen de expresión pública evitando así la coordinación de acciones colectivas[57]. En tal sentido, un informe de la Escuela Central del Partido de 2016 -institución clave en la formación del funcionariado del PCCh- explicita que un entorno informativo parcialmente abierto permite al gobierno detectar precozmente descontento social, anticipar problemas y "resolver eficazmente incidentes de opinión pública". Bajo este sistema de censura poroso, se advierte que parte de la población accede ocasionalmente al contenido sensible; empero, este nunca alcanza la masa crítica, lo que evita la movilización colectiva sin generar un rechazo social equivalente al que produciría una censura total.

Por su parte, China ha integrado tecnologías avanzadas, particularmente algoritmos de IA, sistemas de reconocimiento facial y mega-bases de datos, con el fin de construir uno de los sistemas de

[54] Elizabeth J. Perry, "Cultural Governance in Contemporary China," en *Routledge Handbook of Chinese Governance*, ed. Chris Ogden (London: Routledge, 2020).

[55] Gary King, Pan Jennifer y Roberts, Margaret E, "How Censorship in China Allows Government Criticism but Silences Collective Expression", *American Political Science Review*, 107 n°2 (2013): 326–343.

[56] Accesibles en las bases oficiales de legislación del Comité Permanente de la Asamblea Popular Nacional.

[57] Margaret E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton: Princeton University Press, 2018).

vigilancia más extensos del mundo[58]. Cabe señalar que el país alberga 8 de las 10 ciudades más vigiladas del planeta[59], cuyo monitoreo se legitima oficialmente como herramienta para mantener la seguridad pública y la armonía social. No obstante, numerosos estudios académicos la han caracterizado como un elemento central del autoritarismo digital chino[60].

El sistema de crédito social, inspirado en diversos proyectos piloto y consolidado en documentos oficiales desde 2014, combina datos provenientes de registros policiales y judiciales, información fiscal y sanitaria, comportamiento financiero y actividad en línea. La doctrina ha evidenciado consistentemente[61] que este sistema pretende modelar comportamientos sociales a través de incentivos y sanciones, y se ha calificado internacionalmente como "orwelliano". Sin perjuicio de lo anterior, encuestas internas sugieren que un sector relevante de la población lo percibe como un mecanismo útil para aumentar la seguridad y reducir fraudes[62].

El modelo chino combina elementos propios del autoritarismo digital con rasgos inspirados en los modelos normativos occidentales. China ha manifestado preocupación por el uso excesivo y abusivo de datos personales por parte de las empresas privadas. En este contexto, la Ley de Protección de la Información Personal (*PIPL*, 2021) –también mencionada previamente– incorpora principios similares a los del RGPD de la UE. Entre estos principios compartidos se encuentran la limitación de la finalidad, la minimización de datos, el consentimiento informado, la prohibición de la discriminación algorítmica y los derechos de acceso, rectificación y supresión.

Asimismo, durante sus primeras décadas de expansión digital, China adoptaba un enfoque extremadamente laxo respecto de las empresas tecnológicas nacionales, lo que favorecía su crecimiento acelerado. Esta estrategia remite al "tecnoliberalismo" estadounidense de las décadas de 1990 y 2000. En este sentido, el origen del ecosistema de capital riesgo en China resulta inseparable de la inversión, la asesoría legal y la cultura empresarial importadas desde Silicon Valley[63]. Por ende, los vehículos societarios, incluidos los *offshore* en las Islas Caimán, utilizados para captar inversión extranjera y cotizar en mercados internacionales, se diseñaron por despachos de abogados estadounidenses.

Adicionalmente, la evolución del modelo digital chino no puede comprenderse sin considerar su política industrial proactiva, orientada a convertir a China en una superpotencia tecnológica autosuficiente. De tal modo, esta estrategia se inscribe dentro de un marco más amplio de tecno-nacionalismo, el cual se comprende como la convicción de que el liderazgo tecnológico constituye un requisito indispensable para la seguridad nacional, el desarrollo económico y la proyección geopolítica[64].

En ese orden de ideas, el Gobierno chino ha impulsado la innovación mediante subsidios estatales masivos, inversiones públicas directas, apoyo a empresas de propiedad estatal y mecanismos de planificación estratégica. De tal modo, estudios de la OCDE[65] y del Center for Strategic and International Studies (CSIS) documentan que este país destina cientos de miles de millones de euros a sectores considerados críticos[66].

Por su parte, el presidente Xi Jinping ha afirmado que la autosuficiencia tecnológica es condición indispensable para una "seguridad nacional integral"; en efecto, una noción que aparece

[58] Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras", *New York Times*, 8 de julio de 2018, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html; James Leibold, "Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement", Journal of Contemporary China 29, no. 121 (2019): 46–60.

[59] "The World's Most Monitored Cities", *Comparitech*, 2019, Comparitech.com

[60] Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State", *Journal of Democracy* 30, no. 1 (2019): 53-67.

[61] Wei Dai, "Social Credit: The China Story, Part XIX", *The China Project*, 2019; Yawei Chen, Darrell M. West, y Xiaoqian Sun. "How China's Social Credit System Currently Works: Evidence from Shanghai and Credit China Data". Brookings Institution, 2021.

[62] Genia Kostka, "China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval", *New Media & Society* 21 no. 7(2019): 1565–1593.

[63] Sebastian Mallaby, *The Power Law: Venture Capital and the Making of the New Future* (New York: Penguin Press, 2022).

[64] Segal, "When China Rules...,".

[65] Organisation for Economic Co-operation and Development (OECD), *OECD Science, Technology and Innovation Outlook 2021: Times of Crisis and Opportunity* (Paris: OECD Publishing, 2021).

[66] IA, computación cuántica, robótica avanzada, semiconductores y telecomunicaciones de nueva generación (5G y 6G).

reiteradamente en documentos oficiales del PCCh.

Lanzado en 2015, *Made in China 2025* (MIC2025) es un plan industrial a diez años destinado a transformar a China en líder de la manufactura avanzada. En esa medida, el programa persigue reducir la dependencia de proveedores extranjeros, desarrollar capacidades nacionales en sectores de alto valor tecnológico, fomentar la exportación de productos tecnológicos chinos y apoyar la adquisición de empresas extranjeras con conocimientos especializados. Los subsidios estimados asociados a este programa superan los 300 000 millones de euros[67].

A pesar del rápido avance tecnológico, China mantiene una dependencia significativa respecto a insumos extranjeros clave, especialmente semiconductores. Por ejemplo, en 2019, el país generó aproximadamente el 60 % de la demanda global, pero solo produjo el 13 % de la oferta mundial[68]. En tal sentido, la respuesta oficial ha sido la de establecer un objetivo de autosuficiencia del 70 % para 2025, reforzado por medidas normativas y subsidios. Por lo tanto, se observa que la guerra tecnológica con los EE.UU. -incluyendo restricciones de las dos administraciones Trump y la Biden a la exportación de chips avanzados y equipos de litografía a China- ha intensificado esta estrategia.

Tras la crisis financiera global de 2008, el PCCh integró la innovación tecnológica como pilar de su legitimidad política y como instrumento de modernización económica. En tal sentido, numerosos estudios[69] plantean que la narrativa estatal vincula directamente el progreso tecnológico con el "rejuvenecimiento nacional", un concepto central en la ideología de Xi Jinping.

La estrategia china de desarrollo tecnológico se articula también a través de restricciones sistemáticas al acceso de empresas extranjeras, mecanismos de transferencia forzosa de tecnología y un marco de proteccionismo digital altamente sofisticado. Este proteccionismo digital opera bajo dos lógicas complementarias: por un lado, garantizar el control estatal sobre los flujos de información y, por otro, asegurar la seguridad política y el desarrollo económico.

Durante las décadas de 2000 y 2010, las grandes empresas tecnológicas chinas mantienen una relación simbiótica con el Estado, caracterizada por el apoyo regulatorio a cambio de cooperación en materia de vigilancia y censura. No obstante, este "pacto tácito" se ha visto profundamente alterado. Con posterioridad, la ofensiva regulatoria de China se ha dirigido principalmente a las empresas de software (plataformas digitales, *fintech*, comercio electrónico y juegos en línea), mientras que los sectores de *hardware* estratégico, como los semiconductores, las telecomunicaciones avanzadas o los vehículos eléctricos, quedan relativamente exentos de sanciones.

Esta selectividad pone de manifiesto que el objetivo estatal no consiste en frenar el desarrollo tecnológico, sino en reorientarlo hacia sectores considerados estratégicos para la seguridad nacional y en reducir el poder de intermediación informacional de las grandes plataformas[70].

Ahora bien, una diferencia estructural con Occidente es que ninguna empresa china ha desafiado públicamente al Estado. Asimismo, mientras que Google o Meta han litigado contra autoridades estadounidenses o europeas, empresas como Alibaba o Tencent han respondido a las sanciones millonarias recibidas con declaraciones de aceptación pública de sanciones, compromisos de cumplimiento normativo e incluso reorganizaciones internas alineadas con las prioridades estatales. En consecuencia, este comportamiento refleja tanto el diseño institucional autoritario como los fuertes incentivos económicos de alineación con el PCCh[71].

Así, el nuevo pacto tecnológico implica que el Estado controla el poder estructural del sector digital, y las plataformas aceptan su subordinación y contribuyen a objetivos de redistribución y estabilidad. A cambio, el Estado continúa apoyando sectores estratégicos (hardware, IA, semiconductores); aún así, no tolera concentración de poder que amenace al PCCh.

A pesar de su aparente coherencia, el modelo presenta paradojas significativas. En ese sentido, China demuestra que un ecosistema innovador puede surgir sin libertades políticas amplias, lo que

[67] Jost Wübbeke, Meissner Mirjam, Zenglein Max J., Ives Jaqueline y Conrad, Björn, *Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries* (Berlin: Mercator Institute for China Studies [MERICS], 2016).

[68] Semiconductor Industry Association, *State of the U.S. Semiconductor Industry 2020* (Washington, DC: Semiconductor Industry Association, 2020).

[69] Yongnian Zheng y Lance L. P. Gore, *Technological Innovation and China's Reform: The Dynamics of Change* (London: Routledge, 2022); Elizabeth C. Economy, *The Third Revolution: Xi Jinping and the New Chinese State* (New York: Oxford University Press, 2018).

[70] Segal, *When China Rules the Web*; Scott, *China's Uneven High-Tech Drive*.

[71] Francis Fukuyama, "What Kind of Regime Does China Have?" *Journal of Democracy* 31, no. 1 (2020): 5–20.

contradice la tesis liberal según la cual la innovación depende de un entorno abierto[72]. Sin embargo, quizás debe cuestionarse si esto sería sostenible solo en el corto y medio plazo.

De tal modo, China ha exportado sistemas de vigilancia y gestión de datos a numerosos países (especialmente en África, América Latina, Asia Central y Oriente Medio) a través de proyectos como *Safe Cities* de Huawei[73]. En contextos autoritarios, estos sistemas se utilizan para fortalecer capacidades de control político. Por consiguiente, este país aspira a que su modelo sea una opción atractiva para países con estructuras políticas centralizadas o con débiles instituciones democráticas. Su objetivo –en consonancia con el de la Ruta de la Seda– es exclusivamente introducir sus productos y servicios en dichos países, sin anhelar la exportación de sus cultura y sus valores al mundo.

7. Conclusiones

Desde 1973, prácticamente todos los Estados del mundo han promulgado leyes de protección de datos y privacidad a un ritmo medio de tres nuevas normas nacionales por año. En la actualidad, se encuentran en vigor más de 200 leyes nacionales en esta materia. No obstante, este ritmo legislativo acelerado apenas logra hacer frente a la velocidad creciente con la que evoluciona la tecnología y al consiguiente desarrollo de las oportunidades de negocio internacional.

Puede afirmarse que, en determinados ámbitos, las transacciones digitales superan ampliamente a las analógicas[74]. Así, el comercio digital se ha convertido en el tejido invisible de la economía moderna y de la vida cotidiana. En este contexto, parece evidente que una normativa nacional tradicional por sí sola no puede garantizar un nivel adecuado de protección de los derechos a la protección de datos y a la privacidad en las actividades de tratamiento que incluyen flujos transfronterizos de datos.

De entrada, el comercio y la privacidad constituyen materias dispares que deben mantenerse conceptualmente separadas, puesto que no resulta admisible someter un derecho humano a consideraciones económicas. No obstante, en lo que respecta al derecho a la protección de datos de carácter personal, aun cuando se reconoce como un derecho fundamental, dicha separación no resulta necesariamente evidente en todas las jurisdicciones. Esta situación se observa incluso en las dos principales jurisdicciones en esta materia dentro del marco de las operaciones comerciales —EE. UU. y la UE—. Ambas potencias protagonizan un desarrollo normativo creciente y dinámico en foros comerciales bilaterales y regionales, lo que puede abrir la puerta a ciertos procesos de armonización, sin que ello implique la desaparición de un entorno normativo fragmentado.

De tal modo, EE. UU. se posiciona como el primer exportador mundial de servicios digitales. La Ruta 66, inaugurada en 1926 y convertida en un símbolo cultural estadounidense, ha funcionado históricamente como un eje de movilidad, comercio y proyección identitaria. Esto representa la libertad individual, la expansión económica y el espíritu emprendedor que caracterizan la narrativa del progreso en ese país. De manera análoga, en la actualidad, el ecosistema digital estadounidense constituye una de las principales manifestaciones contemporáneas de ese mismo imaginario: un espacio de innovación acelerada, escasa intervención regulatoria y predominio del mercado como motor organizador. La Ruta 66 y el comercio digital estadounidense comparten, en este sentido, un rasgo definitorio: la centralidad del individuo como agente autónomo.

En el contexto de la Ruta 66, el viajero decidía su recorrido, asumía los riesgos y aprovechaba las oportunidades comerciales que surgían en su trayecto. En el entorno digital contemporáneo, el usuario se conceptualiza de manera similar, como un sujeto libre que decide qué servicios utilizar, qué datos compartir y con qué plataformas interactuar. Sin embargo, esta percepción omite la profunda asimetría informacional que caracteriza al comercio digital. Mientras que los viajeros de la Ruta 66 interactuaban con negocios locales en un entorno económico relativamente equilibrado, el usuario digital actual se enfrenta a empresas cuya capacidad de recopilación y análisis de datos supera ampliamente su entendimiento y su control individual.

Asimismo, este paralelismo se extiende a la forma en que EE. UU. conciben la regulación. La Ruta

[72] Yasheng Huang, *The Rise and Fall of the EAST: Examination, Autocracy, Stability, and Technology* (New Haven: Yale University Press, 2021).

[73] Mozur, "Inside China's Dystopian Dreams".

[74] Por ejemplo, mientras EE. UU. tiene un gran déficit comercial en bienes, tiene un superávit enorme en servicios, especialmente digitales (Déficit en bienes: > USD 900.000 millones, Superávit en servicios: ~ USD 250.000 millones, Superávit digital: ~ USD 240.000 millones). Es decir, los servicios digitales sostienen buena parte del equilibrio comercial de EE. UU.

66 operó durante décadas como un espacio en el que una regulación estatal mínima permitió un florecimiento económico basado en la iniciativa privada. El derecho digital estadounidense reproduce esta tradición, ya que, en lugar de imponer un marco normativo general comparable al de la UE, el país opta por un mosaico de leyes sectoriales (como la *HIPAA* en materia de datos de salud o la *COPPA* respecto de los menores) que fragmentan la protección de los datos personales. En este enfoque, el mercado, más que el Estado, actúa como principal regulador del flujo de información. Si bien este modelo resulta coherente con el *ethos* representado por la Ruta 66 y favorece la competencia y la innovación, sitúa al usuario en una posición de vulnerabilidad estructural.

Del mismo modo, la Ruta 66 funciona como símbolo de movilidad económica y social, al conectar pequeñas poblaciones con grandes mercados. De manera similar, el comercio digital permite que empresas pequeñas y emprendedores accedan a mercados globales mediante servicios basados en datos, posicionándose en un ecosistema de competencia ampliada. Ahora bien, así como la Ruta 66 termina drenando actividad económica hacia grandes conglomerados de autopistas y centros urbanos, el mercado digital estadounidense tiende a favorecer la concentración del poder económico en grandes plataformas tecnológicas, lo que genera nuevas jerarquías que cuestionan el ideal de igualdad de oportunidades.

Desde esta perspectiva, el análisis comparativo entre la Ruta 66 y la concepción estadounidense del derecho del comercio digital pone de manifiesto una continuidad cultural profunda. Ambos configuran espacios de movilidad —física o digital— sustentados en la libertad individual, la mínima intervención estatal y la primacía del mercado como estructura organizadora. Ahora bien, esta analogía permite identificar, al mismo tiempo, las tensiones inherentes a dicho modelo, entre las que destacan la creciente asimetría entre usuarios y empresas, la fragmentación normativa y la concentración del poder económico. Mientras la Ruta 66 simboliza un pasado de oportunidades abiertas, el ecosistema digital estadounidense representa un presente en el que dichas oportunidades coexisten con desafíos legales y éticos que exigen una reflexión más profunda sobre la naturaleza de los datos personales en una sociedad tecnológicamente avanzada.

En contraposición con la Ruta 66, desde la Edad Media el Camino de Santiago constituye un eje de movilidad, intercambio cultural y cooperación entre los territorios europeos. Las rutas jacobeas no solo conectan ciudades y reinos, sino que configuran una red estructurada que garantiza la seguridad, la hospitalidad y la atención al peregrino. Esta red incluye hospitales, albergues y sistemas de señalización que permiten un tránsito relativamente seguro y homogéneo a través de distintas regiones. En este contexto, el peregrino no se desplaza únicamente como individuo aislado, sino que lo hace dentro de un marco normativo y cultural que lo protege y lo integra en una comunidad más amplia. Un proceso similar se observa en la evolución del derecho europeo del comercio digital. Frente al crecimiento exponencial de los servicios digitales y a la centralidad de los datos personales como activo económico, la UE desarrolla un modelo regulatorio orientado a garantizar la protección del usuario y a asegurar un funcionamiento armonizado del mercado digital. Normativas como el RGPD, la DSA o la DMA buscan construir un espacio digital europeo en el que la persona permanece en el centro y en el que la libre circulación de servicios se equilibra con elevados niveles de garantías jurídicas.

En este sentido, el paralelismo más evidente entre ambos fenómenos se encuentra en su función protectora. Así como las rutas jacobeas establecen normas y estructuras destinadas a proteger al peregrino frente a abusos, peligros o situaciones de desamparo, el modelo europeo de regulación digital pretende salvaguardar al usuario frente a los riesgos derivados del tratamiento masivo de datos personales, las asimetrías de poder entre plataformas y consumidores, la opacidad algorítmica o las prácticas comerciales invasivas. Tanto en la peregrinación medieval como en el entorno digital contemporáneo, Europa se concibe a sí misma como garante de una travesía segura.

Además, ambos contextos comparten una clara vocación transfronteriza. El Camino de Santiago ha sido históricamente una red supranacional, capaz de conectar territorios diversos bajo un imaginario común. De manera análoga, la regulación digital europea se concibe para operar más allá de las fronteras estatales, al articular un mercado único de servicios digitales que requiere reglas uniformes para funcionar de manera adecuada. En este sentido, la existencia del denominado "efecto Bruselas" —entendido como la tendencia global a adoptar estándares europeos en materia de privacidad y regulación digital— refuerza la idea de que Europa, al igual que ocurrió con la construcción simbólica del Camino, continúa proyectando modelos normativos más allá de su propio territorio.

En esta línea, la UE, además del modelo de las decisiones de adecuación, ha exportado ampliamente el mecanismo de las cláusulas contractuales tipo a más de 80 Estados, incluidos algunos tan remotos como Arabia Saudí. Con todo, existe una notable disparidad entre los modelos de cláusulas elaborados por dichos Estados terceros, así como entre aquellos facilitados por organizaciones regionales como el Consejo de Europa, la Red Iberoamericana de Protección de Datos o la Asociación de Naciones de Asia Sudoriental (ASEAN). En consecuencia, puede afirmarse que este mecanismo se ha exportado fundamentalmente como concepto, más que como un modelo

normativo homogéneo, relegando su implementación en la práctica.
Para la seguridad y continuidad de las transacciones[75] resulta fundamental la compatibilidad entre los diferentes modelos de cláusulas contractuales tipo. Por lo tanto, la interoperabilidad es necesaria para evitar situaciones en las que los actores (responsables de tratamiento de datos) deben recurrir a distintas cláusulas en función de la transferencia de datos que vayan a realizar (así ocurre, por ejemplo, entre la UE y Asia).

En contraposición con los modelos anteriores -la Ruta 66 y el Camino de Santiago-, la Ruta de la Seda es comparable al enfoque chino ante la privacidad. Ambos sistemas comparten una estructura conceptual: tanto la Ruta de la Seda como la arquitectura digital contemporánea china son mecanismos para consolidar poder, asegurar la estabilidad interna y proyectar influencia internacional. En ese sentido, China entiende los servicios digitales basados en datos personales no solo desde una dimensión económica, sino como elementos esenciales de un nuevo orden global en el que la información reemplaza a las mercancías tradicionales como principal recurso estratégico.

La comparación entre la Ruta de la Seda y la concepción china del derecho del comercio digital pone de relieve una continuidad histórica en la manera en que China entiende la circulación de bienes (materiales o digitales) y su regulación. La gobernanza digital china contemporánea se sustenta en principios que evocan los mecanismos imperiales de control de los flujos comerciales, mediante un enfoque centralizado orientado a la seguridad nacional y a la proyección comercial internacional. En el siglo XXI, los datos personales se configuran como la nueva materia prima de un orden global en transformación y China, en consonancia con la tradición de la Ruta de la Seda, procura asegurar su posición como nodo central en este amplio sistema de intercambios. Por la Ruta de la Seda no transitaban peregrinos ni emprendedores en busca de un futuro mejor, transitaban mercaderes que exportaban sus mercancías al mundo. Del mismo modo, China –en contraste con EE.UU. y la UE– no impregna su estrategia digital de valores ni espiritualidad. Sus objetivos son estrictamente económicos.

Comprender las razones que subyacen a la regulación del entorno digital permite anticipar tanto el impacto de dicha regulación en el mercado como su viabilidad y su capacidad de adaptación en el entorno transfronterizo.

A partir de este escenario, la coexistencia de tres modelos regulatorios diferenciados (EE. UU., UE y China) está dando lugar a una creciente fragmentación global, a menudo descrita como *splinternet*, caracterizada por regímenes jurídicos incompatibles, estándares tecnológicos divergentes y un aumento de los controles geopolíticos sobre los flujos de datos.

Las iniciativas bilaterales y multilaterales podrían, paulatinamente, facilitar la aproximación hacia una regulación equilibrada entre la protección de los datos personales y la flexibilidad para la materialización de los flujos transfronterizos de estos. Al respecto, la OMC continúa negociando sobre "comercio electrónico"[76], mientras que la OCDE, el Consejo de Europa e incluso el Grupo de los Siete (G7) podrían aprovechar su experiencia negociadora en esta materia con el fin de apaciguar las tensiones en torno a la extraterritorialidad de la normativa estadounidense en materia de vigilancia gubernamental. Por el contrario, las tensiones derivadas de la percepción europea sobre la afectación negativa de dicha normativa a los derechos e intereses de los europeos –en determinadas circunstancias– derivan en su incompatibilidad con los términos en que se diseñaron las transferencias internacionales de datos en el RGPD.

En este marco, el modelo chino podría resultar menos problemático al ser coherente con su arquitectura política autoritaria, al priorizar la estabilidad y el control por encima de la libertad individual. La combinación de control estatal, planificación industrial y dinámicas de mercado regulado ha permitido a China consolidarse como una superpotencia tecnológica, desafiando la narrativa liberal que asocia de manera directa la libertad política con el progreso tecnológico. No obstante, las tensiones entre el control estatal y el dinamismo empresarial plantean interrogantes sobre la sostenibilidad de este modelo, especialmente en aquellos sectores que dependen de la innovación disruptiva. Asimismo, la proyección internacional del modelo chino –con sus recientes esfuerzos por flexibilizarse– está reconfigurando el orden digital global, al generar un escenario de competencia normativa con los EE.UU. y la UE. En ese sentido, el futuro del modelo depende de su capacidad para equilibrar seguridad, crecimiento e innovación, en un entorno marcado por una presión geopolítica creciente y una competencia tecnológica acelerada. Por su parte, informes del Banco Mundial de 2022 advierten que una regulación excesivamente punitiva puede reducir

[75] Véase Organisation for Economic Co-operation and Development (OECD), *Moving Forward on Data Free Flow with Trust: New Evidence and Analysis of Business Experiences*, OECD Digital Economy Papers, no. 353 (Paris: OECD Publishing, 2023), 15.

[76] Mozur, "Inside China's Dystopian Dreams".

la productividad en sectores dinámicos. No obstante, también resulta posible concebir sinergias entre los distintos esfuerzos multilaterales que permitan avanzar hacia una arquitectura global de flujos transfronterizos de datos más coherente.

Ante este panorama, EE. UU. y la UE han impulsado estrategias destinadas a frenar la proliferación del modelo chino. Por un lado, EE. UU. aplica la doctrina de la "reciprocidad digital", mediante restricciones a la exportación de tecnologías y la imposición de sanciones a empresas chinas. Por otro, la UE avanza en la construcción de su autonomía digital, fundamentada en la protección de los derechos fundamentales. Ambos actores conciben el modelo chino como un contrapeso normativo que cuestiona los pilares del orden digital liberal. En este sentido, los próximos años pondrán a prueba la voluntad de cooperación internacional en el ámbito de la regulación del comercio digital –y en particular de la economía del dato–. Hasta entonces, el escenario se caracteriza por una situación de *fragile trust*.

Bibliografía

Carrizo, David. "Reflexiones a propósito de la protección de datos en el escenario global digital: El derecho de daños en la litigiosidad internacional." *Revista Boliviana de Derecho*, no. 31 (2021): 445–472.

Chen, Yawei, Darrell M. West y Xiaoqian Sun. "How China's Social Credit System Currently Works: Evidence from Shanghai and Credit China Data." Brookings Institution, 2021.

Comisión Europea. "EU–US Data Privacy Framework: Questions and Answers on the Adequacy Decision." 13 de diciembre de 2022. https://ec.europa.eu/commission/presscorner/detail/de/qanda_22_7632.

Comisión Europea. "Servicios – estadísticas." Acceso el 8 de marzo de 2026. https://trade.ec.europa.eu/access-to-markets/en/content/services-statistics.

Comité Europeo de Protección de Datos (EDPB). *Recomendaciones 02/2020 sobre las garantías esenciales europeas para medidas de vigilancia*. Adoptadas el 10 de noviembre de 2020. https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_es.

Creemers, Rogier. "China's Conception of Cyber Sovereignty: Rhetoric and Realization." En *Governing Cyberspace: Behavior, Power, and Diplomacy*, editado por Dennis Broeders y Bibi van den Berg. Lanham, MD: Rowman & Littlefield, 2020.

Cruz Villalón, Pedro. *Conclusiones del Abogado General en el asunto C-347/10, A. Salemink v Raad van bestuur van het Uitvoeringsinstituut Werknemersverzekeringen*. 8 de septiembre de 2011. ECLI:EU:C:2011:562.

Dai, Wei. "Social Credit: The China Story, Part XIX." *The China Project*. 2019.

Economy, Elizabeth C. *The Third Revolution: Xi Jinping and the New Chinese State*. New York: Oxford University Press, 2018.

Fukuyama, Francis. "What Kind of Regime Does China Have?" *Journal of Democracy* 31, no. 1 (2020): 5–20.

Huang, Yasheng. *The Rise and Fall of the EAST: Examination, Autocracy, Stability, and Technology*. New Haven: Yale University Press, 2021.

Jacques Delors Institute. *Europe in the World: Mapping the EU's Digital Trade—A Global Leader Hidden in Plain Sight?* París: Jacques Delors Institute, 2023.

Kennedy, Scott. *China's Uneven High-Tech Drive: Implications for the United States*. Washington, DC: Center for Strategic and International Studies, 2020.

King, Gary, Jennifer Pan y Margaret E. Roberts. "How Censorship in China Allows Government Criticism but Silences Collective Expression." *American Political Science Review* 107, no. 2 (2013): 326–343.

Kostka, Genia. "China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval." *New Media & Society* 21, no. 7 (2019): 1565–1593.

Kuner, Christopher. "Reality and Illusion in EU Data Transfer Regulation Post Schrems." *German Law Journal* 18, no. 4 (2017): 881–918.

Leibold, James. "Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement." *Journal of Contemporary China* 29, no. 121 (2019): 46–60.

MacKinnon, Rebecca. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books, 2012.

Mallaby, Sebastian. *The Power Law: Venture Capital and the Making of the New Future*. New York: Penguin Press, 2022.

Mistale, Taylor. "Limits That Public International Law Poses on the European Union Safeguarding the Fundamental Right to Data Protection Extraterritorially." En *Transatlantic Jurisdictional Conflicts in Data Protection Law: Fundamental Rights, Privacy and Extraterritoriality*, editado por Taylor Mistale. Cambridge: Cambridge University Press, 2023.

Mozur, Paul. "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras." *New York Times*. 8 de julio de 2018. https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

NOYB – European Center for Digital Rights. "La Comisión Europea da un tercer asalto ante el TJUE a las transferencias de datos entre la UE y EE. UU." 10 de agosto de 2023. https://noyb.eu/es/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

Organisation for Economic Co-operation and Development (OECD). *OECD Science, Technology and Innovation Outlook 2021: Times of Crisis and Opportunity*. Paris: OECD Publishing, 2021.

Organisation for Economic Co-operation and Development (OECD). "Declaration on Government Access to Personal Data Held by Private Sector Entities." *OECD Legal Instruments*. 13 de mayo de 2023. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

Organisation for Economic Co-operation and Development (OECD). *Moving Forward on Data Free Flow with Trust: New Evidence and Analysis of Business Experiences*. OECD Digital Economy Papers, no. 353. Paris: OECD Publishing, 2023.

Organización Mundial del Comercio (OMC). *Acuerdo General sobre el Comercio de Servicios (AGCS)*. 1994.

Otero García-Castrillón, Carmen. *Protección de datos en la economía digital: Una aproximación desde la regulación del comercio internacional*. Pamplona: Thomson Reuters Aranzadi, 2021.

Parlamento Europeo. *Exchanges of Personal Data after the Schrems II Judgment*. Bruselas: Parlamento Europeo, 2021.

Parlamento Europeo y Consejo de la Unión Europea. *Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos)*. DOUE L 119, 4 de mayo de 2016.

Perry, Elizabeth J. "Cultural Governance in Contemporary China." En *Routledge Handbook of Chinese Governance*, editado por Chris Ogden. London: Routledge, 2020.

Qiang, Xiao. "The Road to Digital Unfreedom: President Xi's Surveillance State." *Journal of Democracy* 30, no. 1 (2019): 53–67.

Roberts, Margaret E. *Censored: Distraction and Diversion Inside China's Great Firewall*. Princeton: Princeton University Press, 2018.

Roland, Gérard, y Nancy Qian. "The Evolution of China's Development Strategy." NBER Working Paper no. 29343. Cambridge, MA: National Bureau of Economic Research, 2021. https://doi.org/10.3386/w29343.

Schwartz, Paul M., y Karl-Nikolaus Peifer. "Structuring International Data Privacy Law." *International Data Privacy Law* 9, no. 1 (2019): 7–21.

Segal, Adam. *When China Rules the Web: Technology in Service of the State*. New York: Council on Foreign Relations Press, 2018.

Semiconductor Industry Association. *State of the U.S. Semiconductor Industry 2020*. Washington, DC: Semiconductor Industry Association, 2020.

The White House. "Fact Sheet: Biden-Harris Administration Announces New AI Actions and Receives Additional Major Voluntary Commitments on AI." 26 de julio de 2024.

The Transatlantic Economy 2021: Digital Acceleration. The Transatlantic Economy. 2021. https://transatlanticrelations.org/wp-content/uploads/2021/03/TA-economy-2021_CH4.pdf.

Tribunal de Justicia de la Unión Europea. *Data Protection Commissioner v Facebook Ireland Ltd y Maximillian Schrems*. Asunto C-311/18. Sentencia de 16 de julio de 2020 (*Schrems II*).

Tribunal de Justicia de la Unión Europea. *Maximillian Schrems v Data Protection Commissioner*. Asunto C-362/14. Sentencia de 6 de octubre de 2015 (*Schrems I*).

U.S. Department of Commerce. "EU–U.S. Data Privacy Framework." *Data Privacy Framework Program*. https://www.dataprivacyframework.gov/EU-US-Framework.

United States. *Communications Decency Act*. 47 U.S.C. § 230 (1996).

United States Congress. *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*. S.2383. 115th Cong. 2018.

Unión Europea. *Diario Oficial de la Unión Europea*. L 112. 24 de abril de 2012.

Unión Europea y República de Chile. *Agreement Establishing an Association between the European Community and Its Member States, of the One Part, and the Republic of Chile, of the Other Part*. 2002.

Wübbeke, Jost, Mirjam Meissner, Max J. Zenglein, Jaqueline Ives y Björn Conrad. *Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries*. Berlin: Mercator Institute for China Studies (MERICS), 2016.

Zheng, Yongnian, y Lance L. P. Gore. *Technological Innovation and China's Reform: The Dynamics of Change*. London: Routledge, 2022.