

Flujo de Datos Transfronterizos Translated by Daniel Urbina

*This is the best thing to read on the geopolitical history of the "free flow of data" neoliberal craze. Evgeny Morozov, 7/Dec/2015, on twitter)*

Traducción al Español del artículo: “Transborder Data Flows”; publicado (6/Dic/2015) en:  
[informationobservatory.info/2015/12/06/transborder-data-flows/#\\_edn5](http://informationobservatory.info/2015/12/06/transborder-data-flows/#_edn5)

A inicios de Octubre, la Corte Suprema Europea invalidó el acuerdo vigente hace 15 años conocido como “Puerto Seguro” – un acuerdo internacional que la Unión Europea había negociado con los Estados Unidos para alivianar la Directiva Europea sobre Protección de Datos de 1995 [1] para permitir a las empresas la transferencia de datos personales en formato digital desde la Unión Europea a los Estados Unidos.[2] Representa esta sentencia de la Corte Europea un cambio fundamental en la política digital – un punto final – o simplemente una coma?

Esta es de hecho la reaparición de un conflicto estructural antiguo. Sus orígenes datan de hace casi cincuenta años – cuando los flujos transfronterizos de datos informáticos [FTD] amenazaron con convertirse en un punto de conflicto agudo entre Estados Unidos, Europa, y los nuevos países independientes pertenecientes al entonces denominado Tercer Mundo.

A mediados de los 70s, el FTD era tanto controvertido como inevitable para las agencias militares y empresas de Estados Unidos. En 1981, Herbert I. Schiller mostró como, algunos miles de grandes corporaciones con inversiones extranjeras directas fuera de los Estados Unidos y (dos tercios de ellas) con oficinas centrales en los Estados Unidos – dependían de “un crecientemente abultado flujo de datos circulando *dentro* de [sus] redes comerciales y *a través* de las fronteras nacionales.”[3] Estas empresas pertenecientes a todo tipo de sectores económicos, usaron las primeras redes de comunicaciones computacionales para transmitir datos relativos a todo tipo de operaciones como “inventarios de materias primas, cronogramas de producción, control de calidad, registros de personal, información legal y tributaria, transacciones monetarias, repatriación de utilidades, y decisiones de inversión.” Como subrayó Schiller, el FTD ayudó a las más grandes corporaciones a “efectuar su comercio global tanto como a profundizar la internacionalización del capital.”[4]

Una segunda fuente de FTD fueron las Fuerzas Armadas de Estados Unidos y sus aliados. “La capacidad de las empresas estadounidenses de operar en forma global, explotando recursos y operando en mercados en distintas partes del mundo,” detallaba Schiller, “sería inimaginable sin el completo respaldo de un poder militar concentrado, preparado para un

despliegue e intervención instantáneos.”[5] Las agencias militares y de inteligencia dependían del FTD en red para operar sus bases alrededor del mundo; para coordinar ataques; y para conducir una vigilancia crecientemente más amplia.

No se contó con inventarios exhaustivos de FTD; incluso los arqueos parciales fueron altamente inexactos, dado que los datos fluían, entre territorios, en forma protegida. Cuántos datos era enviados sobre circuitos privados de telecomunicaciones, que eran los que transportaban la mayoría de este flujo? Qué proporción del FTD representaban los datos administrativos y operacionales de empresas? Qué parte del total lo componían datos personales identificables? Qué estaban haciendo las compañías con todos sus datos “propios”? Los estados no se dignaron a investigar. La ausencia de documentación pública significativa revelaba un desequilibrio de poder subyacente. Las grandes empresas insistieron, con éxito, que los encargados de política pública no miraran muy de cerca los FTD, por temor que dicha investigación condujera a llamados a aumentar la rendición de cuentas (accountability) – lo que habría podido restringir las operaciones de sus proyectos de márgenes exitosos.

El FTD no sólo confirió poder sobre el capital corporativo, sino también, paradójicamente, estableció un nuevo punto de vulnerabilidad para el mismo. Las interrupciones y requisitos de supervisión pusieron en peligro la economía política que estaba siendo reconstruida en torno a las comunicaciones informáticas. Aparecieron amenazas físicas derivadas de terremotos o incluso derivadas del arrastre de una ancla de barco que pudiera romper un cable submarino a través del cual circulaban datos; sin embargo, lejos más importante para las grandes empresas eran las amenazas políticas, derivadas de iniciativas dirigidas a restringir el contenido del FTD, o de establecer cargos por volumen de datos enviados, o de la supervisión del FTD con fines de autogobierno.

Los flujos transfronterizos de datos aún no se habían convertido en un aspecto positivo, aunque de bajo perfil, de lo que pasaría a llamarse la “globalización.” De hecho, desde el final de los años 70s y por algunos años, pareció posible – incluso probable – que los FTD estallarían como una controversia internacional de alto nivel. El primer factor fue la experiencia del Nazismo en el recuerdo de los europeos, que instaló una sana desconfianza por la captura y almacenamiento de datos computacionales, y que acentuó la percepción de la necesidad de proteger la privacidad en un contexto emergentemente tecnologizado. Esto motivó la introducción de legislación de protección de datos en Alemania, Suecia, Francia y Dinamarca a inicios de los 70s,[6] en la cual la privacidad fue conceptualizada como un derecho humano fundamental que requiere protección contra riesgos de abuso asociados el almacenamiento centralizado de datos (en ese entonces en computadores “mainframe”).

La segunda motivación estuvo asociada a la búsqueda por parte de empresas y gobiernos europeos de instancias para hacer frente a lo que un alto oficial francés había llamado “el desafío de Estados Unidos” en materia de alta tecnología.[7] A finales de los 70s y principios de los 80s, esta preocupación se intensificó. Algunos altos dignatarios europeos se preocuparon de las capacidades de red que permitirían a Estados Unidos actuar como una

especie de “OPEC de la Información.”[8] Por medio de limitar el FTD desde y hacia los Estados Unidos, los encargados de política pública europeos esperaban crear un espacio para contrarrestar el poder de información creciente de los Estados Unidos – al mismo tiempo de establecer sus propias capacidades en materia de software y redes de comunicaciones.

Finalmente, un aún activo proyecto político nacido en el Tercer Mundo también comenzó a apuntar al FTD, el que fue visto como una extensión de la dominación de Occidente en aspectos tecnológicos y culturales. A medida que los llamados a la protección de datos ganaron relevancia política, empezó a emerger un desafío importante al poder global de Estados Unidos.[9]

El tema del FTD se intensificó por tanto. En el curso de tres años, observó Schiller, “a mitad de los 80s, 24 países, la mayoría, pero no todos de Europa, habían puesto en vigencia legislación de protección de datos o estaban en alguna fase preparatoria para hacerlo.”[10] El movimiento político para reforzar la protección de datos, en si mismo representaba una dificultad adicional para el capital transnacional, puesto que se generó un contexto de regulaciones nacionales divergentes que complejizó e hizo más costoso hacer negocios en múltiples territorios.

Los responsables de política pública en Estados Unidos rápidamente identificaron lo que estaba en juego. El Senador Barry Goldwater, Jr., en una sesión sobre flujo de datos internacionales ante un sub-comité del Comité Senatorial sobre Operaciones de Gobierno estableció que “estamos viendo la emergencia de legislación nacional de privacidad que representa de hecho la aparición de nuevas barreras al comercio... Han descubierto que el simple pacto que bloquear el flujo de datos en el año 1980, significa bloquear el comercio.”[11] Las compañías estadounidenses, desde el sector manufactura a la banca al sector tecnológico protestaron ardientemente contra regular el FTD. En esta misma sesión, Motorola testificó que “la existencia de más controles y regulaciones sobre nuestras comunicaciones podrían forzar a nuestras subsidiarias a instalar sistemas específicos o contratar servicios locales. El riesgo es que estas alternativas sean demasiado costosas o lentas para efectos de mantener la competitividad en el mercado y en último término, pondrían en riesgo la libertad para operar de la manera más eficiente a nivel mundial.”[12] Es decir, estaba en juego nada menos que la internacionalización del capital.

Cambiando desde la defensiva a la ofensiva a fines de los 70s, el gobierno de los Estados Unidos enfrentó estas amenazas trasladando la formulación de políticas fuera del contexto de Naciones Unidas y hacia un entorno más amistoso como el provisto por la Organización para la Cooperación y el Desarrollo Económico (OCDE) – un club compuesto por la élite de los países de mayores ingresos. En 1980, la OCDE comenzó un proceso paralelo para hacer más específica y armónica la regulación sobre protección de datos. Las Guías sobre Privacidad que emitió en 1980 encontraron una creciente adhesión en la política europea, la cual la Unión Europea formalizó en su directiva de Protección de Datos de 1995.

A lo largo de las décadas finales del siglo 20, algunos cambios estructurales ayudaron a reforzar la posición estadounidense en FTD. Utilizando los garrotes del poder económico y militar en contra del Tercer Mundo, durante los 80s, Estados Unidos re-dirigió las preocupaciones de los países menos desarrollados en torno al FTD mostrándoles la zanahoria de la “tecnología para el desarrollo.” Más redes resolverían el problema de la dominación estructural. Adentrándose en los 90s, maravillosos cambios en conectividad se produjeron con la coyuntura que también vio la caída del socialismo soviético; la reinserción de China en el capitalismo global; y la firma del Tratado de Maastricht, que estableció a la Unión Europea con una Alemania reunificada en el centro. Los líderes estadounidenses trabajaron para posicionar la emergente internet en este contexto fundamentalmente diferente, como un símbolo de libertad individual y como una herramienta de la “sociedad civil” para manifestarse frente al estado abusivo. La UE armonizó su política de protección de datos, y en el 2000 adoptó el procedimiento del “puerto seguro”. Esto creó lo que RAND Corporation llamaría “un mercado común Europeo para el libre movimiento de los datos personales”[13] y – no coincidentemente – también permitió a las grandes compañías estadounidenses con operaciones en Europa el envío de flujos digitales de información personal de vuelta a los Estados Unidos para su procesamiento. El mecanismo del Puerto Seguro fue concebido mediante la ficción diestramente compartida de la inexistencia de amenazas para los derechos de privacidad de los europeos. El logro esencial fue remover un obstáculo potencialmente significativo a la expansión vinculada a las redes por parte de las empresas capitalistas que dominaban el FTD.

Los sistemas de comunicaciones computacionales florecieron en forma recíproca. Se sobreponían la ejecución de procesos de extensión, expansión y transformación tecnológica.

Cuando Herbert Schiller escribió su texto, menos de un tercio de los países participaban en el sistema de FTD.[14] Hoy en cambio, después de asombrosos desarrollos de infraestructura, las organizaciones en casi todos los países interactúan a través de redes – aunque con grandes disparidades en el volumen de flujos de datos entre las naciones. La ruta más fuertemente traficada, hoy como en 1980, es aquella entre Estados Unidos y Europa Occidental[15]; sin embargo, casi todas las rutas transoceánicas son más densamente usadas que en el pasado. La cantidad de ancho de banda adicional puesto en servicio en 2014, esto es, la capacidad adicional de transporte de mensajes asociada a los cables submarinos mundiales, es comparable a casi la capacidad completa de banda ancha que estaba disponible mundialmente en 2011.[16] La capacidad de los circuitos disponibles para tráfico de datos ha aumentado, para hacer frente a la tan publicitada “convergencia” que permite que videos, textos, imágenes, voz y datos puedan ser transportados en un flujo común de bits.

Cambios actuales en la economía política han modulado mejoramientos en la tecnología de redes. Por una parte, el mercado capitalista se ha globalizado en forma genuina. Así como China, los países miembros de la ex Unión Soviética, y participantes por vez única en el proyecto político del Tercer Mundo todos se reintegraron al capitalismo global, el FTD enlazó unidades de capital operando a nivel mundial. Por otra parte, cambios en la propiedad y control de las redes las han transformado en plataformas de propósito general en un proceso

acelerado de comoditización de la información. Con la llamada liberalización y privatización, durante los 80s y 90s, las redes que habían sido interconectadas a través de servidores centralizados operados por ministerios gubernamentales migraron a redes que interconectan las locaciones de empresas en forma directa. La Internet es por lejos la más completa expresión de esta tendencia. La proporción de FTD que corresponde a exportaciones e importaciones de commodities derivadas de datos ha crecido proporcionalmente. Desde el 2007 al 2011 – años de crisis económica – las exportaciones estadounidenses de servicios digitales crecieron de \$282.1 billones a \$356.1 billones.[17] En 2012, las exportaciones estadounidenses entregadas en-línea a la UE alcanzaron un valor de \$140 billones.[18]

Durante las décadas que han pasado desde los 80s, por lo tanto, el FTD se ha generalizado. Como característica esencial y común de las operaciones globales de las grandes empresas, y un sistema de distribución de commodities globales, el FTD ha sido naturalizado tan profundamente hasta llegar a desaparecer como objeto de análisis crítico. Muy por el contrario, contemplamos un sinfín de reverencias a la doctrina del libre flujo de la información, como si esta doctrina estuviera libre del interés propio de las corporaciones. El proceso de subsumir el FTD como el conducto del capitalismo transnacional es cada vez más profundo y ocurre casi sin inspección, y debe ser contado como un éxito político espectacular del capital estadounidense, en particular.

Lo que nos lleva a la sentencia dictada el 6 de Octubre, por la Corte Europea de Justicia. La Corte vinculó su hallazgo – que los datos personales de los europeos no están protegidos contra abusos al ser transferidos a Estados Unidos – a las revelaciones de Edward Snowden sobre la vigilancia masiva llevada a cabo por la Agencia Nacional de Seguridad estadounidense.[19] Esta decisión es como una llave inglesa lanzada directamente a los engranajes giratorios del capitalismo digital.

La razón radica en que un nuevo ciclo de cambio técnico organizacional en torno a las redes, está ganando velocidad rápidamente. En el marco de los últimos seis o siete años, smartphones e innumerables sensores, detectores, sondas y otros dispositivos nuevos para la captura de datos han comenzado a implantar conectividad en cada uno de los poros de la economía política. La arquitectura de las redes está mutando hacia datacenters privados y centros de intercambio de tráfico privados para impulsar estos datos dinámicos. Los flujos de datos, principalmente compuestos de flujos de datos personales, son cada vez más continuos y omnipresentes. Este desarrollo de lugares pone cada vez más presión en la actual – y ya insuficiente – política de protección de datos, en la que Estados Unidos, el líder en “datificación”, ya ni siquiera participa. Cuando “los datos personales son continuamente levantados, aumentados, corregidos, intercambiados y re-usados,”[20] decía un estudio de RAND Corporation en 2009, los riesgos de abuso son “bastante mayores”. Aún así, al inicio del 2010, el Departamento de Comercio estadounidense inició una investigación dirigida a identificar barreras a la reestructuración técnica de redes, al mismo tiempo que trabajaba para (como lo dijera Google en sus comentarios) “asegurar que los servicios puedan ser provistos sin inversión local ni infraestructura.”[21] Es decir, una vez más estamos en un momento re-integrativo, cuando los Estados Unidos como el representante de los grandes capitales está

tratando de armonizar estándares internacionales más permisivos para el FTD. Al moverse en contra de esta corriente, la Corte Europea de Justicia en forma prospectiva abrió la puerta a los temas de la rendición de cuentas y control asociados al FTD.

Se escucharon voces de protesta, y poco después del veredicto, el Congreso estadounidense agendó audiencias sobre la decisión europea del “puerto seguro” y su impacto en los flujos de datos transatlánticos.[22] En dichas audiencias, las compañías estadounidenses exigieron urgentemente a su gobierno tomar acción para restaurar aquellos flujos de datos transatlánticos libres de obligaciones. Jeffrey Immelt, CEO de General Electric – que está tratando de empujar la “Internet de las Cosas” (IoT) y la que segurá elevando la importancia de los flujos de datos – se pronunció en contra de invalidar el acuerdo de Puerto Seguro antes de que anunciara la sentencia.[23] Aunque Google y Facebook son los mayores afectados a simple vista por la sentencia europea, no menos de 4400 corporaciones serán impactadas.[24] Si la sentencia se ratifica, empresas de otros rubros además de las del sector tecnológico tendrán que reorganizar sus operaciones como: Recursos Humanos, pago de sueldos, logística y administración de la cadena de suministros.

Estados Unidos por su parte empezó a presionar por *mayor* libertad para invertir, *por menos* protección de la privacidad, y por *mas amplia* armonización legal mucho antes de la que tinta de la decisión de la Corte Europea se hubiera secado. Esto es evidente del texto del TPP (Transpacific Trade Partnership) que se negoció en secreto – que consiste en un acuerdo comercial entre Estados Unidos y otros 11 países con costa en el Océano Pacífico.[25] El artículo 10.6 del capítulo de Comercio de Servicios Transfronterizos, de dicho acuerdo, establece que “las Partes no exigirán a los proveedores de servicio de las otras partes signatarias, establecer o mantener oficinas de representación o cualquier tipo de empresa, o exigir residencia, en su territorio como condición para la prestación de un servicio a través de fronteras.”[26] El artículo 14.11 del capítulo de Comercio Electrónico, establece que las partes “deberán permitir el flujo de información transfronterizo por medios electrónicos, incluyendo información personal, para efectos de actividad comercial de personas jurídicas”; aún sí, permite a los signatarios adoptar o mantener “medidas inconsistentes” con la obligación anterior cuando se refiere a “alcanzar un objetivo legítimo de política pública” – y siempre que el hacerlo no constituya una “discriminación arbitraria o injustificable o una restricción comercial encubierta.”[27] Contraviniendo preceptos claves de la decisión de “Puerto Seguro” de la UE, estos artículos efectivamente van más allá hasta evitar que los países miembros puedan bloquear el FTD o demandar la localización de los datos – aunque el tratado deja algún espacio a otros miembros para desafiar a Estados Unidos en caso de sentirse motivados a hacerlo. Al tratar el FTD como una lógica comercial, sin embargo, el acuerdo sitúa al FTD en un ámbito que está saturado de intereses de capital más que por sinceras preocupaciones por la democracia política.

La presión será ciertamente intensa para trasladar el articulado que favorece a los negocios del FTD desde el TTP hacia su contraparte: la aún secreta negociación del Transatlantic Trade and Investment Partnership (TTIP), entre Estados Unidos y la Unión Europea. La Comisión Europea ha dispuesto un plazo de tres meses para desarrollar una alternativa al



acuerdo de “Puerto Seguro”, y Washington y Bruselas han estado “encerrados en arduas negociaciones – de intensidad creciente,” y muestra de ello es el intento de llegar a un nuevo acuerdo para FTD a través de conversaciones directas entre Joe Biden, Vice Presidente estadounidense y el Jefe Ejecutivo de la Unión Europea Jean-Claude Juncker.<sup>[28]</sup> El punto en discordia, de acuerdo a informaciones de prensa, es “cuánto más acceso” a los datos personales de ciudadanos europeos, permitir a las agencias de inteligencia estadounidenses.

Como vemos, el FTD sigue siendo vulnerable a cambios políticos tanto como lo fue en 1980. El conflicto gira en torno tanto a la rivalidad económica y, especialmente, al “derecho” de los militares para invadir la vida política y social. Cabe esperar que la decisión de la Corte Europea consiga ser el primer paso hacia un movimiento de oposición que impida incursiones militares en la gobernanza democrática. Pero tal vez no debiésemos ser tan optimistas.

## REFERENCIAS

[1] La Directiva de Protección de Datos mandata que, en conformidad con la Carta Europea de Derechos Fundamentales, la transferencia de datos personales a otro país puede verificarse solo si dicho país asegura un nivel de protección de privacidad adecuado de dicha información. Este compromiso se materializa a través de leyes locales o “compromisos internacionales”. El acuerdo de Puerto Seguro se utilizó como forma de compromiso internacional para permitir a las empresas el envío de flujos digitales de información personal desde países miembros de la UE a los Estados Unidos.

[2] [The Court of Justice declares that the Commission’s US Safe Harbour Decision is invalid](#), Press Release, Court of Justice of the European Union.

[3] Herbert I. Schiller, *Who Knows: Information in the Age of the Fortune 500* (Norwood: Ablex, 1981), 101.

[4] Schiller, *Who Knows*, 101.

[5] Schiller, *Who Knows*: 106.

[6] *The Politics of Transborder Data Flows: Competing Values, Interests, and Institutions*

[7] Jean-Jacques Servan-Schreiber, *The American Challenge*. New York: Scribner, 1968.

[8] [International Data Flow: Hearings before a Subcommittee of the Committee On Government Operations](#), House of Representatives, Ninety-Sixth Congress, Second Session, March 10, 13, 27, and April 21, 1980. Washington: U.S. G.P.O., 1980.

- [9] Eileen Marie Mahoney, “Negotiating New Information Technology and National Development: The Role of the Inter-Governmental Bureau for Informatics,” Ph.D. Diss., Temple University, 1987.
- [10] Schiller, *Who Knows*: 162.
- [11] [International Data Flow: Hearings before a Subcommittee of the Committee On Government Operations](#), House of Representatives, Ninety-Sixth Congress, Second Session, March 10, 13, 27, and April 21, 1980. Washington: U.S. G.P.O., 1980.
- [12] Frank Kuitenbrouwer, *The World Data War*, *New Scientist*, September 3, 1981
- [13] Neil Robinson, Hans Graux, Maartin Botterman, Lorenzo Valeri, “[Review of the European Data Protection Directive](#).” Santa Monica: RAND Corporation, 2009: 7.
- [14] Schiller, *Who Knows*: 101, citing *Datamation* March 1978: 203.
- [15] Accounting by one estimate for roughly 55% of total TDF. Joshua Meltzer, “[Examining the EU safe harbor decision and impacts for transatlantic data flows](#),” *Brookings*, November 3, 2015.
- [16] “Global Network Construction Resurgence,” *TeleGeography*, April 23, 2015.
- [17] United States International Trade Commission, “[Digital Trade in the US and Global Economics, Part 1](#),” July 2013.
- [18] National Foreign Trade Council, “[Promoting Cross-Border Data Flows: Priorities for the Business Community](#).”; Jessica Nicholson and Ryan Noonan, “[Digital Economy and Cross Border Trade: The Value of Digitally- Deliverable Service](#),” U.S. Department of Commerce, 2014.
- [19] Mark Scott, “[European Court Advisor Calls Trans-Atlantic Data-Sharing Pact Insufficient](#),” *New York Times*, September 24, 2015; Mark Scott, “[U.S.-Europe Data Transfer Agreement Is Ruled Invalid](#),” *New York Times*, October 7, 2015.
- [20] Neil Robinson, Hans Graux, Maartin Botterman & Lorenzo Valeri, “[Review of the European Data Protection Directive](#),” Santa Monica: RAND Corporation, 2009: 7.
- [21] Google, Inc., [Comments to the Department of Commerce, Notice of Inquiry on the Global Free Flow of Information on the Internet](#): 13-14 ; See Dan Schiller, *Digital depression: information technology and economic crisis*(Urbana, Chicago : University of Illinois Press), 170-84.



[22] Hearing: Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows, Subcommittee on Communications and Technology (Committee on Energy and Commerce), November 3, 2015.

[23] Richard Waters, "[Jeff Immelt warns EU data curbs could limit productivity gains](#)," *Financial Times*, October 1, 2015: 23.

[24] Cameron Kerry, "[Safe Harbour invalidation puts EU data in quarantine](#)," *euObserver*, October 26, 2015.

[25] "[Trans-Pacific Partnership \(TPP\): More Job Offshoring, Lower Wages, Unsafe Food Imports](#)," *Public Citizen*.

[26] Chapter 10: [Cross Border Trade in Service](#).

[27] Chapter 14: [Electronic Commerce](#).

[28] Duncan Robinson, "[Transatlantic safe harbor deal still months away, EU warns](#)," *Financial Times*, November 5, 2015.