

Instituto de la Judicatura del Poder Judicial del Estado de Nuevo León

Maestría en Argumentación Judicial

*Reconstrucción argumentativa de la sentencia del Tribunal de Justicia (Gran Sala)  
de 16 de julio de 2020. TJUE, Data Protection. Commissioner v. Facebook Ireland y  
Schrems (C-311/18)*

Docente: Dr. Rogelio López Sánchez

Materia: Teoría Jurídica Contemporánea y Argumentación Jurídica

Alumno: Licenciado Filemón Soto Marín

Monterrey, Nuevo León a de mayo de 2026.

**Reconstrucción argumentativa de la sentencia del Tribunal de Justicia (Gran Sala) de 16 de julio de 2020. TJUE, Data Protection. Commissioner v. Facebook Ireland y Schrems (C-311/18)**

Antes de entrar propiamente al análisis y nota crítica de la sentencia de referencia, es importante señalar que en la lectura del Capítulo 3 denominado EL DERECHO HUMANO A LA PROTECCIÓN DE DATOS PERSONALES Y DESAFÍOS ANTE LAS NUEVAS TECNOLOGÍAS, contenido en el libro: “EL DERECHO A LA INFORMACIÓN Y DATOS PERSONALES EN MÉXICO, UNA VISIÓN COMPARADA CON EL SISTEMA INTERAMERICANO Y EUROPEO DE DERECHOS HUMANOS, en sus páginas 97 a la 132), el suscrito advertí que se destaca el derecho fundamental a la protección de datos personales y la eficacia de los derechos frente a particulares, también de cómo en las últimas décadas ha sido asombrosa la evolución del derecho a la privacidad de los datos de carácter personal y que el derecho al honor e intimidad constituyen un elemento esencial de la dignidad humana y libre desarrollo de la personalidad y que el uso de la informática constituía uno de los mayores riesgos para la intimidad individual y familiar. Destaca el texto que hoy en día el manejo de datos personales ha dado un viraje sorprendente, esto debido a la revolución informática que los coloca en el umbral del escrutinio público y ejemplo las redes sociales y los buscadores digitales en las que más allá del morbo social generado por la publicidad de nuestras vidas, lo verdaderamente importante es la vulneración al derecho a la intimidad, principalmente de los datos personales en el acontecer diario, a través de la publicidad de nuestros datos por grandes corporativos, tanto nacionales como internacionales, cuyo objeto comercial, lo es precisamente el procesamiento de datos, lo que significa la ruptura de un paradigma en el que los derechos fundamentales también sean sujetos de protección en contra de violaciones cometidas por particulares, pues aunque los contratos celebrados entre particulares, buscan lograr el principio de la autonomía de la voluntad, ineludiblemente conducen también a restricciones a la autonomía individual de los derechos, los cuales deben ser sujetos de la tutela y protección de esa libertad al momento de celebrar una relación contractual ante cualquier corporativo o empresa, entre otras, financiera, de relaciones públicas o de contratación, dado que éstas forzosamente adquieren el compromiso de no afectar los derechos fundamentales de sus consumidores o prestadores de servicios.

Es así como a raíz de las transformaciones y cambios tecnológicos, el reconocimiento progresivo del derecho a la privacidad de los datos personales en comento, ha aumentado su umbral de protección hasta crear nuevos derechos y garantías, como la protección de tales datos personales, a partir de conflictos entre particulares.

Como antecedentes de los aludidos conflictos, en contra de particulares, por violar la privacidad e intimidad de las personas, especialmente cuando se trata de datos personales tenemos los de Alemania, Francia, Bélgica y otras naciones europeas, por ejemplo, el texto señala que se sancionó a la empresa Google por la captación y almacenamiento de datos personales de miles de usuarios a través de su herramienta Street View, ya que captaban los datos de las redes inalámbricas instaladas tanto en lugares públicos como en los domicilios de miles de personas. Asimismo, cita que en México también se han realizado reclamos de parte del IFAI, en contra de grandes corporativos como Sony de México SA de CV, quien sufrió un ataque cibernético por haber sido sustraídos diversos datos personales, como nombre, dirección ciudad, Estado, código postal, país, dirección de correo electrónico, sexo, fecha de nacimiento, número de teléfono, nombre de usuario y contraseñas, al igual que posible información crediticia; igualmente, que en nuestro país es común la venta y distribución comercial de bases de datos en el mercado negro, situación de alarma que motivó el debate en la elaboración de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Por todo lo anterior, es que en México y en otros países se han generado leyes para la protección de los datos personales, sobre todo tratándose de la categoría de datos sensibles, ya que ello provoca que se agrave la multa impuesta por la autoridad a los particulares, teniendo como antecedente criterios jurisprudenciales del derecho alemán y español, al definir estos datos como aquellos que puedan revelar aspectos como el origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencia sexual.

Otro aspecto relevante que considera el texto es que la piedra angular de futuras interpretaciones sobre los alcances y restricciones al derecho fundamental de protección de datos, es el principio de proporcionalidad, que nos remite a los 12 y 13, de la citada Ley en el sentido de que el tratamiento de datos personales se limitará al cumplimiento de las finalidades previstas en el aviso de privacidad y no para un fin distinto que no resulte compatible o análogo a los fines convenidos, y que en particular cuando se trate de datos personales sensibles, se deberán realizar esfuerzos razonables para limitarlos hasta el mínimo indispensable.

De igual modo el texto plantea el caso de Max Schrems, un estudiante irlandés de 24 años, acerca del poder que tiene Facebook sobre nuestros datos personales es bastante delicado, lo que sí es claro es que existen serias deficiencias en el cumplimiento a las leyes de datos personales, ya que después de 22 reclamaciones ante el organismo irlandés de

protección de datos, obligó a que la empresa Facebook le entregara a Schrems un CD con datos personales con más de mil páginas, donde se encontraban datos acumulados en tres años, incluidas conversaciones que él mismo había borrado, pero que seguían conservadas en archivos digitales, situación que es cada vez más frecuente, pues actualmente en numerosos países existen agencias de recursos humanos que buscan detalladamente datos personales de sus empleados a través de medios digitales, tratando de hurgar el pasado oscuro de sus posibles empleados.

**Ahora bien, en cuanto a la reconstrucción argumentativa de la sentencia del Tribunal de Justicia (Gran Sala) de 16 de julio de 2020.**

Respecto a las **premisas fácticas**, tenemos que en esta sentencia versa sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales en el asunto C-311/18, por la High Court (Tribunal Superior, Irlanda), entre Data Protection Commissioner y Facebook Ireland Ltd, Maximillian Schrems, con intervención de The United States of America, Electronic Privacy Information Centre, BSA Business Software Alliance Inc., Digitaleurope.

Los hechos en debate estriban en que el 25 de junio de 2013, el Sr. Schrems presentó ante el Comisario una reclamación en la que en esencia solicitó que prohibiera a Facebook Ireland transferir sus datos personales a los Estados Unidos, alegando que el Derecho y las prácticas en vigor en ese país no garantizaban una protección suficiente de los datos personales conservados en su territorio frente a las actividades de vigilancia llevadas a cabo en dicho país por las autoridades públicas, tal reclamación fue desestimada.

Así las cosas, el Tribunal Superior, Irlanda, ante la que el Sr. Schrems había interpuesto un recurso contra la desestimación de su reclamación, planteó al Tribunal de Justicia una petición de decisión prejudicial relativa a la interpretación y a la validez de la Decisión 2000/520 y mediante sentencia el Tribunal de Justicia declaró inválida la referida Decisión

A raíz del fallo anterior, el órgano jurisdiccional remitente anuló la desestimación de la reclamación del Sr. Schrems y se la devolvió al Comisario, en el marco de la investigación abierta por este último, Facebook Ireland explicó que una gran parte de los

datos personales se transfería a Facebook Inc. basándose en cláusulas tipo de protección de datos recogidas en el anexo de la Decisión CPT. Habida cuenta de esos elementos, el Comisario instó al Sr. Schrems a modificar su reclamación.

En su reclamación modificada, el Sr. Schrems alegó, en particular, que el Derecho estadounidense obliga a Facebook Inc. a poner los datos personales que se le transfieren a disposición de las autoridades estadounidenses, como la National Security Agency (NSA) y la Federal Bureau of Investigation (FBI). Esgrimió que no puede justificar la transferencia de esos datos a los Estados Unidos, solicitando al Comisario que prohibiese o suspendiese la transferencia de sus datos personales a Facebook Inc.

Posteriormente, el Comisario publicó un proyecto de decisión en el que se resumían las conclusiones provisionales de su investigación y consideró con carácter provisional que los datos personales de ciudadanos de la Unión transferidos a Estados Unidos corrían el riesgo de ser consultados y tratados por las autoridades estadounidenses, sin vincular a las autoridades estadounidenses.

Luego, el Comisario inició un procedimiento ante el High Court, a efectos de que esta última preguntara al Tribunal de Justicia acerca de esta cuestión y la High Court planteó la presente petición de decisión prejudicial ante el Tribunal de Justicia Europea, adjuntando una sentencia en la que había reseñado el resultado del examen de las pruebas que se le habían aportado en el marco del procedimiento nacional, procedimiento en el que había participado el Gobierno estadounidense, en esa sentencia el órgano jurisdiccional remitente señaló que, en principio, no solo tiene el derecho, sino también la obligación de examinar la totalidad de los hechos y argumentos invocados ante ella para decidir, basándose en ellos, si una remisión prejudicial es necesaria o no; en cualquier caso, señaló, que estaba obligado a tener en cuenta las posibles modificaciones del derecho que tuviesen lugar entre la interposición del recurso y la vista que se organizase ante él. Dicho órgano jurisdiccional precisó que, en el marco del procedimiento principal, su propia apreciación no se limitaba a los motivos de invalidez invocados por el Comisario, sino que también podía plantear de oficio otros motivos de invalidez y, basándose en ellos, proceder a una remisión prejudicial.

Asimismo, FISA, el órgano jurisdiccional remitente en la misma sentencia, precisa que se permite al Fiscal General y al Director de los Servicios de Inteligencia Nacionales autorizar conjuntamente, previa aprobación del FISC, con el fin de obtener información en

materia de inteligencia exterior, la vigilancia de personas no nacionales de los Estados Unidos que se encuentren fuera del territorio de ese país y sirve, en particular, de fundamento a los programas de vigilancia PRISM y Upstream. En el marco del programa PRISM, los proveedores de servicios de Internet están obligados, según las apreciaciones del referido órgano jurisdiccional, a proporcionar a la NSA todas las comunicaciones enviadas y recibidas por un selector, de las cuales una parte se transmite también al FBI y a la Central Intelligence Agency (CIA) (Agencia Central de Inteligencia).

En lo que se refiere al programa Upstream, el citado órgano jurisdiccional ha observado que, en el marco de este programa, las empresas de telecomunicaciones que explotan la red troncal de Internet es decir, la red de cables, conmutadores y enrutadores están obligadas a permitir a la NSA copiar y filtrar los flujos de tráfico de Internet con el fin de recabar comunicaciones enviadas o recibidas por el nacional no americano al que corresponda un «selector» o que estén relacionadas con esa persona. En el marco de ese programa, conforme a las apreciaciones de ese mismo órgano jurisdiccional, la NSA tiene acceso tanto a los metadatos como al contenido de las comunicaciones de que se trate.

El órgano jurisdiccional remitente observa que esta permite a la NSA acceder a datos en tránsito hacia los Estados Unidos, accediendo a los cables submarinos situados en el lecho del Atlántico, así como recabar y conservar esos datos antes de que lleguen a los Estados Unidos y estén sujetos a las disposiciones de la FISA. El órgano jurisdiccional remitente precisa que las actividades basadas en la E.O. 12333 no se rigen por la ley.

Por lo que atañe a los límites establecidos con respecto a las actividades de inteligencia, el órgano jurisdiccional remitente pone de relieve el hecho de que a las personas que no son nacionales de Estados Unidos únicamente se les aplican las actividades de inteligencia y basándose en estas apreciaciones, el antedicho órgano jurisdiccional considera que los Estados Unidos llevan a cabo un tratamiento de datos en masa, sin garantizar una protección.

En relación de las **premisas normativas** del citado fallo, tenemos que en el mismo se invocaron los artículo 45, apartado 1, primera frase, 46, apartados 1 y 2, letra c), del RGPD, y que este último numeral debe interpretarse en el sentido de que las garantías adecuadas, los derechos exigibles y las acciones legales efectivas requeridas por dichas disposiciones deben garantizar que los derechos de las personas cuyos datos personales se transfieren a un país tercero sobre la base de cláusulas tipo de protección de datos gozan de

un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión por el referido Reglamento, interpretado a la luz de la Carta. A tal efecto, la evaluación del nivel de protección garantizado en el contexto de una transferencia de esas características debe, en particular, tomar en consideración tanto las estipulaciones contractuales acordadas entre el responsable o el encargado del tratamiento establecidos en la Unión y el destinatario de la transferencia establecido en el país tercero de que se trate como, por lo que atañe a un eventual acceso de las autoridades públicas de ese país tercero a los datos personales de ese modo transferidos, los elementos pertinentes del sistema jurídico de dicho país y, en particular, los mencionados en el artículo 45, apartado 2, del referido Reglamento.

Asimismo, que el artículo 58, apartado 2, letras f) y j), del RGPD debe interpretarse en el sentido de que, a no ser que exista una decisión de adecuación válidamente adoptada por la Comisión, la autoridad de control competente está obligada a suspender o prohibir una transferencia de datos a un país tercero basada en cláusulas tipo de protección de datos adoptadas por la Comisión cuando esa autoridad de control considera, a la luz de todas las circunstancias específicas de la referida transferencia, que dichas cláusulas no se respetan o no pueden respetarse en ese país tercero y que la protección de los datos transferidos exigida por el Derecho de la Unión, en particular, por los citados artículos 45 y 46 del RGPD y por la Carta, no puede garantizarse mediante otros medios, si el responsable o el encargado del tratamiento establecidos en la Unión no han suspendido la transferencia o puesto fin a esta por sí mismos.

Se establece que es inherente al carácter contractual de las cláusulas tipo de protección de datos que estas no pueden vincular a las autoridades públicas de países terceros, pero que a la luz de la interpretación de los artículos 44 y 46, apartados 1 y 2, letra c), del RGPD, exigen que el nivel de protección de las personas físicas garantizado por dicho Reglamento no se vea comprometido, puede resultar necesario completar las garantías recogidas en esas cláusulas tipo de protección de datos. A ese respecto, el considerando 109 del referido Reglamento dispone que «la posibilidad de que [los] responsable[s] [...] del tratamiento recurran a cláusulas tipo de protección de datos adoptadas por la Comisión [...] no debe obstar a que los responsables [...] añadan otras cláusulas o garantías adicionales» y precisa, en particular, que «se debe alentar a los responsables [...] a ofrecer garantías adicionales [...] que complementen las cláusulas tipo de protección de datos».

Se indicó que, por tanto, resulta evidente que las cláusulas tipo de protección de datos adoptadas por la Comisión en virtud del artículo 46, apartado 2, letra c), del mismo

Reglamento tienen únicamente como finalidad proporcionar a los responsables o encargados del tratamiento establecidos en la Unión garantías contractuales que se apliquen de manera uniforme en todos los países terceros y, que independientemente del nivel de protección garantizado en cada uno de ellos. En la medida en que esas cláusulas tipo de protección de datos no pueden proporcionar, debido a su naturaleza, garantías que vayan más allá de una obligación contractual de velar por que se respete el nivel de protección exigido por el Derecho de la Unión, tales cláusulas pueden necesitar, en función de cuál sea la situación de un país tercero determinado, la adopción de medidas adicionales por parte del responsable del tratamiento con el fin de garantizar el respeto de ese nivel de protección.

A este respecto, el mecanismo contractual previsto en el artículo 46, apartado 2, letra c), del RGPD se basa en la responsabilización del encargado del tratamiento establecidos en la Unión, así como, con carácter subsidiario, de la autoridad de control competente y que corresponde, por tanto, ante todo, a ese responsable o encargado del tratamiento comprobar, caso por caso y, si es preciso, en colaboración con el destinatario de la transferencia, si el Derecho del tercer país de destino garantiza una protección adecuada, a la luz del Derecho de la Unión, de los datos personales transferidos sobre la base de cláusulas tipo de protección de datos, proporcionado, cuando sea necesario, garantías adicionales a las ofrecidas por dichas cláusulas.

También que el responsable o el encargado del tratamiento establecidos en la Unión no pueden adoptar medidas adicionales suficientes para garantizar esa protección, estos o, con carácter subsidiario, la autoridad de control competente están obligados a suspender o poner fin a la transferencia de datos personales al país tercero de que se trate. En particular, eso es lo que ocurre cuando el Derecho de ese país tercero impone al destinatario de una transferencia de datos personales procedentes de la Unión obligaciones que son contrarias a las referidas cláusulas y que, por tanto, pueden poner en entredicho la garantía contractual de un nivel de protección adecuado contra el acceso de las autoridades públicas del mencionado país tercero a esos datos.

Y que en este contexto, el artículo 4 de la Decisión CPT, interpretado a la luz del considerando 5 de la Decisión de Ejecución 2016/2297, confirma que en modo alguno la Decisión CPT impide a la autoridad de control competente suspender o prohibir, en su caso, una transferencia de datos personales a un país tercero basada en las cláusulas tipo de protección de datos recogidas en el anexo de dicha Decisión. A este respecto, tal como se desprende de la respuesta a la octava cuestión prejudicial, a no ser que exista una decisión de adecuación válidamente adoptada por la Comisión, la autoridad de control competente



está obligada, en virtud del artículo 58, apartado 2, letras f) y j), del RGPD, a suspender o prohibir esa transferencia cuando considere, a la luz de las circunstancias específicas de la referida transferencia, que dichas cláusulas no se respetan o no pueden respetarse en ese país tercero y que la protección de los datos transferidos exigida por el Derecho de la Unión no puede garantizarse mediante otros medios, si el responsable o el encargado del tratamiento establecidos en la Unión no han suspendido la transferencia o puesto fin a esta por sí mismos.

De lo anterior se desprende que la Decisión CPT prevé mecanismos efectivos que permiten en la práctica garantizar que la transferencia a un país tercero de datos personales sobre la base de las cláusulas tipo de protección de datos recogidas en el anexo de la antedicha Decisión se prohíba o suspenda cuando el destinatario de la transferencia no cumpla las referidas cláusulas o no le resulte posible cumplirlas

**Y como conclusión, se declaró que:**

1 En las normas invocadas en este punto resolutivo de la sentencia, está comprendida una transferencia de datos personales realizada con fines comerciales por un operador económico establecido en un Estado miembro a otro operador económico establecido en un país tercero, a pesar de que, en el transcurso de esa transferencia o tras ella, esos datos puedan ser tratados por las autoridades del país tercero en cuestión con fines de seguridad nacional, defensa y seguridad del Estado.

2 El artículo 46, apartados 1 y apartado 2, letra c), del Reglamento 2016/679 debe interpretarse en el sentido de que las garantías adecuadas, los derechos exigibles y las acciones legales efectivas requeridas por dichas disposiciones deben garantizar que los derechos de las personas cuyos datos personales se transfieren a un país tercero sobre la base de cláusulas tipo de protección de datos gozan de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión Europea por el referido Reglamento, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea. A tal efecto, la evaluación del nivel de protección garantizado en el contexto de una transferencia de esas características debe, en particular, tomar en consideración tanto las estipulaciones contractuales acordadas entre el responsable o el encargado del tratamiento establecidos en la Unión Europea y el destinatario de la transferencia establecido en el país tercero de que se trate como, por lo que atañe a un eventual acceso de las autoridades públicas de ese país tercero a los datos personales de ese modo transferidos,

los elementos pertinentes del sistema jurídico de dicho país y, en particular, los mencionados en el artículo 45, apartado 2, del referido Reglamento.

3. El artículo 58, apartado 2, letras f) y j), del Reglamento 2016/679 debe interpretarse en el sentido de que, a no ser que exista una decisión de adecuación válidamente adoptada por la Comisión Europea, la autoridad de control competente está obligada a suspender o prohibir una transferencia de datos a un país tercero basada en cláusulas tipo de protección de datos adoptadas por la Comisión, cuando esa autoridad de control considera, a la luz de todas las circunstancias específicas de la referida transferencia, que dichas cláusulas no se respetan o no pueden respetarse en ese país tercero y que la protección de los datos transferidos exigida por el Derecho de la Unión, en particular, por los artículos 45 y 46 del mencionado Reglamento y por la Carta de los Derechos Fundamentales, no puede garantizarse mediante otros medios, si el responsable o el encargado del tratamiento establecidos en la Unión no han suspendido la transferencia o puesto fin a esta por sí mismo

4. El examen de la Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, en su versión modificada por la Decisión de Ejecución (UE) 2016/2297 de la Comisión, de 16 de diciembre de 2016, a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales no ha puesto de manifiesto la existencia de ningún elemento que pueda afectar a la validez de dicha Decisión.

5. La citada Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EE. UU., es inválida.

### **Opinión del suscrito.**

Considero que indiscutiblemente este tipo de resoluciones internacionales permean el respeto al derecho humano a la protección de datos personales y desafíos ante las nuevas tecnologías sobre todo tratándose de la categoría de datos sensibles (origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencia sexual), ante posibles

violaciones por parte de particulares, entre otros, empresas, redes sociales buscadores digitales, etcétera.

Sin embargo, los avances en este tema siguen siendo insuficientes para lograr la debida protección de tales datos, esto debido a que fallos como el que nos ocupa con un efecto tan inmediato que obliga a los responsables de la protección de datos a evaluar minuciosamente la legislación y las políticas de cada Estado a cuyas empresas pretendan transferir datos, basándose criterios que tampoco dejó claros el TJUE, al dejar en manos de particulares el tratamiento de los datos la evaluación del nivel de protección de terceros países los obliga a conocer en profundidad su legislación y sus políticas, trasladándoles grandes responsabilidades y dando lugar a opiniones dispares entre unas empresas y otras, lo que obliga así, a las autoridades de control estatales a revisar a su vez las conclusiones a las que llegan los responsables del tratamiento.

Además, que se debe recordar que este análisis genera en los particulares grandes costos y habrá entidades que no dispongan de departamentos especializados en protección de datos.

Por ende, sería más acertado, que la propia autoridad estableciera instrucciones claras y comunes para los diferentes Estados, unificando así el criterio a seguir por las empresas al efectuar transferencias de datos e implementar garantías que permitan el cumplimiento de las exigencias del RGPD.

## REFERENCIAS

1. López Sánchez, R. (2018). El derecho a la información y datos personales en México, una visión comparada con el sistema interamericano y europeo de derechos humanos (pp. 97-132). Dykinson.

2. Tribunal de Justicia de la Unión Europea. (16 de julio de 2020). Sentencia del Tribunal de Justicia (Gran Sala), asunto C311/18, Data Protection Commissioner v Facebook Ireland Limited y Maximilian Schrems [Schrems II]. ECLI:EU:C:2020:559