عبد الرحمن جمال يعقوب
قاضٍ بمجلس الدولة - ماجستير جامعة كامبريدج - ماجستير جامعة ليون ٣

قراءة في حكم محكمة العدل الأوروبية في قضية شريمز ٢ بشأن نقل البيانات الشخصية من الاتحاد الأوروبي إلى الولايات المتحدة الأمريكية

المراسلة: عبد الرحمن جمال يعقوب
مجلس الدولة– مصر

معرف الوثيقة الرقمي (DOI): https://doi.org/10.54873/jolets.v3i1.116

البريد الإلكتروني: Abdelrahman.gamal1@yahoo.com

نسق توثيق البحث:
عبد الرحمن جمال يعقوب، قراءة في حكم محكمة العدل الأوروبية في قضية شريمز ٢ بشأن نقل البيانات الشخصية من الاتحاد الأوروبي إلى الولايات المتحدة الأمريكية، مجلة القانون والتكنولوجيا، المجلد الثالث، العدد الأول، أبريل ٢٠٢٣، صفحات

المقدمة:

إن البيانـات الشخصيـة أصبحت بمثابـة الوقود لكثير من الأنشطـة التجارية الآن. فبالإضافـة إلى الحـالات التي يتوجـب الاحتفاظ فيهـا بالبيانـات الشخصية للعملاء لمباشرة النشاط التجاري ذاته، تقوم الآن الكثير من النماذج التجارية على الاتجار في البيانات الشخصية عينها. فكثير من الخدمات الإلكترونية ومواقع التواصل الاجتماعي والتطبيقات والألعاب وخلافهم الكثير -خاصةً من يقدمون خدماتهم مجانًا- يعتمدون في جزء كبير من نشاطهم على جمع البيانات الشخصية لعملائهم، كلٌ بحسب نشاطه ونوعيـة البيانات التـي يجمعها، لبيعهـا لشركات أخـرى تستخدمها لدراسـة الأسواق وتسويـق منتجاتها بشـكل أفضل. والأمر كذلك في كافة المجـالات التي تتطلب التعامل مـع جمهور تقريبًا؛ فنجد أنه حتى السياسيين يستعينون بخدمات محللي البيانات لفهم القواعـد الانتخابية والوصول إلى أفضل طريقة دعاية انتخابية، مما يعزز فرصهم في الفـوز كما كان الحال في قضية كامبريدج أناليتيكا مثـلًا. لذلك فالبيانات الشخصية أضحت عمادًا اقتصاديًا رئيسيًا، لا يقل الاهتمام به عن الاهتمام بصناعة الطاقة مثلًا.

لا يتصـور مـع اتساع قاعـدة تجارة البيانات علـى هذا النحو أن تغلـق كل دولة على بيانـات مواطنيها داخـل حدودهـا، فالبيانات بحكم تطـور وسائل الاتصـال أصبحت بطبيعتها عابرة للحدود. لذلك فقد تنبهت الكثير من الدول لأهمية وضع تنظيم قانوني محكـم لنقل البيانات إلى الخـارج. في طليعة هذه التنظيمات يأتـي الاتحاد الأوروبي، والذي أنزل قيودًا على عمليات نقل البيانات إلى خارج الاتحاد، تستهدف أن تتمتع هذه البيانـات بذات المستوى من الحمايـة الذي يتيحه قانون الاتحـاد الأوروبي. ولأجل هذا تبنـى الاتحاد الأوروبي آليات حصرية يمكن من خـلال ضمان تحقيق هذا المستوى من الحماية.

تتركز عمليات نقل البيانـات الشخصية للأوروبيين إلى خارج الاتحاد الأوروبي على معيـار أول ورئيسي يتمثل في التساوي بين مستوى حماية البيانات في الاتحاد الأوروبي ذاتـه ووفقًـا لما يكفله قانونه، وبين مستوى حماية البيانـات الذي سيتوافر عند نقل هذه البيانـات للخـارج. وبالرغم من أن عملية نقـل البيانات قد تستنـد إلى أكثر من وسيلة قانونيـة مما يتيحه قانـون الاتحاد الأوروبـي، إلا أن العامل المشـترك بينهم جميعًا هو ذلك المعيار. وفي ظل مستوى الحماية المساوي هذا تواتر قضاء محكمة العدل الأوروبية

موضحًا ما الذي يعنيه، وكيف يمكن للدولة التي تستقبل البيانات أن تعجز عن توفيره.

لقد أصدرت محكمة العدل الأوروبية حكمها في القضية المعروفة إعلاميًّا بـ شريمز ٢ (Schrems II) في ١٦ يوليو ٢٠٢٠، والذي انتهت فيه إلى إبطال قرار الملائمة (Adequacy Decision) لنقل البيانات الشخصية لمواطني الاتحاد الأوروبي إلى الولايات المتحدة الأمريكية المسمى درع الخصوصية (Privacy Shield)، والذي كان يمثل الغطاء القانوني الرئيسي لعمليات نقل البيانات بين الكيانين وما يتبعهم من شركات ومؤسسات على اختلاف الأنشطة والمجالات. وقد كان سبب المحكمة فيما توصلت إليه هو أن القانون الأمريكي لا يكفل الحماية مستوى حماية مكافئ لذلك الخاص بقانون الاتحاد الأوروبي، إذ يخول برامج المراقبة التي تستخدمها أجهزة الأمن الأمريكية سلطات من شأنها انتهاك خصوصية البيانات الشخصية لمواطني الاتحاد الأوروبي. إلا أن المحكمة لم تقض ببطلان البنود التعاقدية القياسية (Standard Contractual Clauses) السارية آنذاك، والتي تمثل إحدى أهم الأدوات البديلة لإعطاء المشروعية لنقل البيانات. لكنها مع ذلك قدرت أن البنود القياسية غير كافية بذاتها، وأنها يجب أن تشتمل على ضمانات أقوى بما يوفر مستوى حماية مساوٍ لمستوى حماية اللائحة العامة لحماية البيانات الخاصة بالاتحاد الأوروبي

(GDPR) General Data Protection Regulation).

ويمثل هذا الحكم إعادة تأكيد من قبل محكمة العدل الأوروبية على التزامها بحماية البيانات الشخصية لمواطني الاتحاد، وعدم استعدادها للتنازل عندما يتعلق الأمر بحماية البيانات الشخصية في مواجهة الدول الأجنبية التي قد تحوز هذه البيانات لأسباب التجارة أو غيرها. لذلك نراها تعيد الكرة من جديد بعد أن أبطلت قبلها بحوالي خمس سنوات قرار الملاءمة للولايات المتحدة الملاذ الآمن (Safe Harbour)، ولأسباب بعضها متكرر. إن الحكم الحالي قد وضع الطرفين الأوروبي والأمريكي في مأزق، إذ إن التوفيق بين المتطلبات المترتبة عليه والتنظيم القانوني الأمريكي يتطلب تغييرًا في القوانين الأمريكية. لذلك لا عجب أن الطرفين لم يتمكنا من إصدار قرار ملاءمة بديل إلى الآن.

إن الحكم لم يؤد بطبيعة الأمر إلى تعطل حركة التجارة الضخمة العابرة للأطلنطي،

إلا أنـه تـرك الشركات الأمريكيـة المتعاملة في البيانـات الشخصيـة الأوروبية لبدائل قانونيـة أخرى لتوفر الغطـاء القانوني لنقل البيانات، إلا أنهـا ليست بذات الدرجة من الاستقـرار والثقـل، ولا توفر ذات الأمـان الذي تكفله قرارات الملاءمـة كوسيلة قانونية رئيسية لنقل البيانات الشخصية إلى خارج الاتحاد.

تأتي على رأس هذه الوسائل البنود التعاقدية القياسية، والتي يمكن لناقلي البيانات تبنيهـا في عقودهـم والالتزام بما تحويه بنودها في صـورة تعاقدية. ذلك وقد تناولت المحكمـة بالبحث صحة قرار البنود التعاقدية القياسية الصادر عن المفوضية الأوروبية (European Commission) والسـاري آنذاك. لكن المحكمة قررت في هذا الصدد أن البنـود القياسيـة ذاتها صحيحة، إلا أن مدى صحة تطبيقهـا يختلف باختلاف الحالة، وهـو ما قد يتطلـب تدعيمها بتدابير إضافية مـن قبل المتحكم أو المعالـج الذي يصدر البيانـات. وعلى هذا الأساس أصبحت البنود التعاقدية القياسية هي الأساس الرئيسي الذي تستند إليه عمليات نقل البيانات منذ ذلك الحين.

يحـاول التعليق الحالي سبر أغوار هذا الحكم من خلال وضعه موضعه في الصورة الأكبر للتنظيم القانوني لنقـل البيانات في الاتحاد الأوروبي، ومن خلال فهم مدلولات قـرار المحكمة بشأنه، وكذلك تحليل أهم نتائجه. لذلك سيتناول التعليق الوقائع وسياق القضيـة أولًا، ثم تحليل الحكـم، فالتعقيب على الحكم، وأخيرًا يختتـم بعرض النتائج التي توصل إليها.

أولًا - الوقائع وسياق القضية:

١- الوضع قبل شريمز ٢:

إن حكـم شريمز ٢ الصادر عن محكمة العدل الأوروبية تكمن أهميته في أنه أسقط اتفاقيـة نقل البيانات بين الاتحـاد الأوروبي ودولة بحجم الولايـات المتحدة وما لها من استثمـارات فـي دول الاتحاد، ومـا يترتب على ذلك مـن تعرية عمليات نقـل البيانات للولايـات المتحدة مـن الغطاء القانوني الأكبر، متمثلًا في قـرار الملاءمة، إلا من بدائل غير مستدامـة ومرهقة مثل قواعد الشـركات الملزمـة (Binding Corporate Rules) والبنـود التعاقدية القياسية. لكن هذه ليست الحادثـة الأولى من نوعها، وإنما سبقها- بوقـت ليس ببعيـد- حكم صدر عن المحكمـة نفسها في عام ٢٠١٥ فـي قضية خاضها

الشخص نفسه، وفي سياق شبيه عرفت إعلاميًّا بـ شريمز ١، ترتب عليها آنذاك بطلان اتفاقية نقل البيانات السابقة الملاذ الآمن (Safe Harbour).[١] وهو ما يجعل من قضية شريمز ٢ حلقة في سلسلة تطورات قانونية وقضائية بخصوص النقل الدولي للبيانات الشخصية في الاتحاد الأوروبي.

محاولات ماكس شريمز - تسريبات إدوارد سنودن ٢٠١٣:

إن مشعل فتيل القضيتين، ومن عرفت القضيتان إعلاميًّا باسمه، هو ماكسيميليان شريمز (Maximilian Schrems)، محامي أيرلندي عنى بقضايا الخصوصية، والتفت منذ باكر إلى تأثير منصة مثل فيس بوك على خصوصية البيانات الشخصية للأوروبيين، حيث يتم نقل بياناتهم لمعالجتها في الولايات المتحدة حيث يوجد مركز الشركة الأم. حرك شريمز العديد من الشكاوى ضد فيس بوك منذ عام ٢٠١١،[٢] لم تؤت أيٌّ منها ثمارها، وكانت هذه الشكاوى تستهدف النظر في مدى التزام فيس بوك بـ «الملاذ الآمن» حيث ادعى أن نقل البيانات إلى الولايات المتحدة غير قانوني ويخالف كلاً من توجيه خصوصية البيانات الأوروبي[٣] (Data Protection Directive Directive 95/ 46/CE1)-)، وكذلك اتفاقية الملاذ الآمن، حيث يتم نقل البيانات دون ضرورة لذلك ودون أن يكفل القانون الأمريكي مستوى حماية للبيانات الشخصية مكافئ لذلك الأوروبي.[٤] ذلك وقد كانت المفوضية الأيرلندية إما تتجنب أو ترفض هذه الشكاوى تحت ادعاءات مختلفة، منها: أنها غير ملتزمة قانونًا بالنظر في هذه الشكاوى وأن السلطات الوطنية لا يحق لها نقض قرارات المفوضية الأوروبية.[٥]

كانت حادثة إفشاء التنصت العالمي التي قام بها إدوارد سنودن (Edward Snowden) خبير المعلومات الذي عمل لصالح وكالة الأمن القومي الأمريكية بمثابة الغيث من السماء لقضية شريمز التي عانت من جفاف الإهمال، كما كانت هي ذاتها

(1) (Schrems I) Case C-364/14 Maximillian Schrems v Data Protection Commissioner, [2015] CJEU.

(٢) قدم ما يجاوز العشرين شكوى يوجد حصر بها على الموقع الإلكتروني الخاص به والذي أسسه مزامنة مع بدء حركته ضد انتهاكات الخصوصية من فيس بوك، [http://europe-v-facebook.org/EN/Complaints/Safe_Harbor/safe_harbor.html]، الزيارة الأخيرة ١٥/٩/٢٠٢٢م.

(٣) تم استبداله عام ٢٠١٨ باللائحة العامة لحماية البيانات الشخصية، وهي السارية حاليًا، والتي تم بحث قضية شريمز ٢ في ضوئها.

(٤) [http://www.europe-v-facebook.org/prism/facebook.pdf]، الزيارة الأخيرة ١٥/٩/٢٠٢٢م.

(5) Alvarez D, "Safe Harbor Is Dead; Long Live the Privacy Shield?" [2016] Business Law Today 5.

صدمة للرأي العام العالمي برمته. ذلك أن بعض المنصات الصحفية مثل الجارديان ونيويورك تايمز نشرت عام ٢٠١٣ وثائق تكشف تورط وكالة الأمن القومي الأمريكية وشركاء لها في عمليات تنصت عالمي وعلى نطاق واسع طالت مواطنين أمريكيين وغير أمريكيين، من بينهم أوروبيون، كشفها لهم إدوارد سنودن عبر آلاف الوثاق المسربة التي تثبت ذلك وتوضح الوسائل التي تم اتباعها في التنصت[١].

عقب تلك التسريبات لجأ شريمز للمحكمة الأيرلندية العليا، والتي قبلت الدعوى ضد المفوضية الأيرلندية وتبنت رواية شريمز، إذ قدرت أنه ولإن كانت معالجة البيانات تتم لحماية الأمن القومي، إلا أنها تفتقد إلى القانونية من حيث إنه تتم معالجة بيانات عدد كبير من المواطنين بشكل جماعي وغير مميز. لكن لما كانت هناك اتفاقية نقل بيانات بين الاتحاد الأوروبي والولايات المتحدة -الملاذ الآمن- والتي دخلت حيز التنفيذ بقرار المفوضية الأوروبية رقم ٢٠٠٠/٥٢٠، وهو ما يخرج من اختصاصها أن تنظره، فقد أقرت المحكمة العليا أن في عملية نقل البيانات تلك انتهاكًا للدستور الأيرلندي، ووقفت نظر الدعوى وأحالتها لمحكمة العدل الأوروبية بصفتها المختص بنظر القضايا المنصبة على قوانين الاتحاد الأوروبي.

حكم محكمة العدل الأوروبية في شريمز ١:

أحالت المحكمة العليا الأيرلندية قضية ماكس شريمز ضد المفوضية الأيرلندية لحماية البيانات لمحكمة العدل الأوروبية على أن تنظر سؤالين:[٢]

السؤال الأول: وهو أساس النزاع بين طرفي القضية، كان: هل إصدار المفوضية الأوروبية قرار ملاءمة لصالح إحدى الدول، إعمالًا للمادة (٢٥) من توجيه حماية البيانات يكف يد السلطات الإشرافية الوطنية (The supervisory authority) عن نظر شكاوى الأفراد المنصبة على مستوى حماية البيانات في هذه الدولة؟

وبالنسبة لهذا السؤال فقد أشارت المحكمة إلى أنه من حيث المبدأ يحق للمفوضية الأوروبية لحقوق الإنسان، وكذلك للدول الأعضاء، أن يعتبروا قوانين حماية البيانات

(١) وقد شملت عمليات التنصت تلك وسائل اتصال مختلفة مثل الرسائل النصية والبريدية والمحادثات الهاتفية، [https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded]، الزيارة الأخيرة ٢٠٢٢/٩/١٠م.

(٢) قضية رقم C-٣٦٢/١٤ أمام المحكمة العليا الأيرلندية، حكم الإحالة، الفقرتان ١٩، ٢٢.

فـي دولـة معينة متناسبة مـع مستوى حماية الاتحـاد الأوروبي،[١] إلا أنـه إذا أصدرت المفوضيـة قـرارًا بذلك، فإنه لا يحق للـدول الأعضاء ولا مؤسساتهـم مخالفته بإصدار أيـة قـرار يعتبر مستوى الحماية غـير كاف، وأن ذلـك مبناه أن المفوضيـة شأنها شأن مؤسسـات الاتحاد الأوروبي يفترض في القرارات الصـادرة عنها الصحة والنفاذ إلى أن يتـم سحبهـا أو إلغاؤها أو إصدار حكم ببطلانهـا.[٢] ومع ذلك، فإن هذا لا يحد من حـق الأفراد الذيـن تنقل بياناتهم للخارج من أن يتقدموا بشكـوى للسلطات الإشرافية حتـى وإن كانـت المفوضية قد أصدرت قـرارًا بملاءمة القوانين في البلـد المنقول إليها البيانـات من قبل، ولا هـو يتعارض مع الاختصاص الأصيل للسلطـات الإشرافية في تلقي الشكاوى من الأفراد، والتي منحت إليها بموجب اتفاقية الاتحاد الأوروبي، وتوجيه حماية البيانات[٣].

السـؤال الثـاني: وقـد أحالته المحكمـة دون أن يكون مثـارًا للنزاع أمامهـا، وهو هل اتفاقية الملاذ الآمن، وبالتحديد قرار اعتمادها الصادر عن المفوضية الأوروبية، يتوافق مع توجيه حماية البيانات الساري آنذاك؟ وذلك السؤال يثير مسألة موضوعية.

وفيما يتعلق بهذا السؤال، فقد أثارت محكمة العدل سؤالًا ثانويًا مفاده: ما هو المقصود بالمفهـوم الذي ورد في المادة (٢٥) من توجيه حماية البيانات من أن تكون الحماية في الدولـة المنقـول إليها البيانات مكافئة لذلك في الاتحـاد الأوروبي؟ وبخصوصه أجابت المحكمة بأن التوجيه لم ينص على تعريف لهذا المفهوم، لا في تلك المادة ولا غيرها. إلا أن الحكـم يستطرد بأنه بقراءة نص المـادة ذاته يتضح أن المستوى الملائم من الحماية يقتضـي أن يتحقـق للدولة المنقول لهـا البيانات بموجب قوانينهـا أو التزاماتها الدولية مستـوى ملائـم من حمايـة البيانات، وأن يقاس ذلك بمنظار حمايـة الحياة الخاصة والحقوق والحريات الأساسية للأفراد[٤].

فيمـا يخص مفهوم «الملاءمـة» ذاته، فإنه لا يفترض أن يكـون مستوى الحماية في الدولـة المنقول إليهـا البيانات «مطابقًا» لنظـيره في الاتحاد الأوروبـي، وإنما يعني أن تضمـن تلك الدولـة حماية للحقوق والحريـات الأساسية متلائمًا فـي جوهره مع ذلك الذي يكفله توجيه حماية البيانات[٥].

(1) Schrems I, para 50.
(2) Ibid, para 52.
(3) Ibid, para 57.
(4) Schrems I, paras 70-71.
(5) Ibid, para 73.

ومـن هذا المنطلق بحثـت المحكمة التسـاؤل الرئيسي متمثلًا فيمـا إذا كان مستوى الحمايـة فـي القانـون الأمريكي ملائمًـا أم لا، وبالنظـر في حكمها نجـد أن المحكمة استندت إلى مبدأي الضرورة والوضوح في حكمها النهائي ببطلان قرار اعتماد اتفاقية المـلاذ الآمن، وإن لم تشر لهما صراحـةً. وأما الأول فمقتضاه ألا يتم اللجوء إلى تدابير مـن شأنها تقييد حقوق وحريـات الأفراد إلا بقدر ما تقتضيه ضـرورة الموقف، والثاني يتطلـب أن تكون القيود الممكن توقيعها مبنية على قواعد محددة الملامح والأبعاد بحيث يمكـن للأفـراد معرفة تبعـات أفعالهم، وأن تقـترن بضمانات تكفل عـدم التعسف في توقيعها[١]. حيث تذكر المحكمة أنه يجب أن تكون هناك قواعد واضحة ومحددة لمعالجة البيانات علـى أن يصاحبها ضمانات ضد المعالجة غير القانونية، وتصبح تلك الحاجة ملحة بالنسبة للبيانات المعالجة إلكترونيًا[٢].

وبناءً على ذلـك تذهب محكمة العدل إلى أن التشريع (تقصد بذلك قرار المفوضية باعتمـاد اتفاقية المـلاذ الآمن) الذي يسمح بنقل بيانات إلى الخارج بدون تمييز أو قيد أو استثنـاء، وبدون معيار محـدد للبيانات التي يمكن نقلهـا أو الغرض من نقلها، يكون مقوضًـا للحق فـي احترام الحياة الخاصـة المنصوص عليه في المـادة (٧) من ميثاق الحقـوق الأساسية للاتحاد الأوروبي[٣]. كما اعتبرت أن عدم النص على آلية للتظلم أو طلـب تعديل أو حـذف البيانات هو انتهاك كذلك للحق فـي الخصوصية[٤]. وعلى تلك الأسس قضت المحكمة ببطلان المادة (١) من الملاذ الآمن – أي ببطلانه ذاته.

وبالإضافة إلى ذلك فقد قضت المحكمة ببطلان المادة الأولى من القرار لعيب شكلي يتمثـل فـي أن المفوضية في قرار الملاءمة يجب أن تعلـن أن الدولة المزمع نقل البيانات لهـا تضمن مستوى ملائمًا من الحماية، وهو لم يشمله القرار رقم ٢٥٠-٢٠٠٠ باعتماد المـلاذ الآمن[٥]. ولما كانت المحكمة قد رأت أن المادة (٣) هي الأخرى باطلة؛ لأنها تمنح المفوضيـة الأوروبية القدرة علـى تقييد اختصاص السلطـات الإشرافية الوطنية بدون

---

(١) يمكن استنتاج أن المحكمة تستوحي رأيها ذلك من الاختبار ثلاثي الخطوات الذي يترسخ في أحكامها وأحكام محكمة حقوق الإنسـان الأوروبيـة والذي يوجب أن يكون القيد على أحد الحقوق أو الحريـات مؤسسًا على قانون واضح ودقيق، وأن يستهدف مصلحة مشروعة، وأن يكون الإجراء المقيد للحق في استجابة لضرورة يفرضها الواقع ومتناسبًا مع حجم تلك الضرورة.

(2) Schrems I (n 1), paras 91-92.

(3) Ibid, paras 93 – 94.

(4) Ibid, para 95.

(5) Ibid, paras 99 – 103.

سنـد سليـم، وأن المادتين (١ و٣) تمسان بدورهما غيرهما مـن المواد، فقط انتهت إلى بطلان القرار برمته، وبالتالي اتفاقية الملاذ الآمن.

ويمكـن تفسير هذا القرار على أنـه خطوة منطقية بالنظر إلى التغيرات التي طرأت خلال خمسة عشر عامًا هي مدة تطبيقه، وفوقها سنوات الإعداد،[١] فالولايات المتحدة قـد مـرت بتفجير برجي التجـارة العالميين، ومـا ترتب على ذلك مـن اتخاذها لتدابير تستهـدف مـن ورائها تعزيز أمنها القومـي، مثل تمريـر Patriot Act الذي يطلق أيدي سلطاتها الأمنية في جمع البيانات.

٢- شريمز ٢: مقدمات الحكم:

لقـد أعقب إبطال المـلاذ الآمن صدور اللائحة العامة لحمايـة البيانات في ٢٠١٦، ومـن ثَمَّ دخوله حيز النفاذ في ٢٠١٨، وفي العام ذاته ٢٠١٦ انتهت المفوضية الأوروبية ووزارة التجارة الأمريكية إلى الاتفاق على إطار جديد لنقل البيانات من الاتحاد الأوروبي إلى الولايـات المتحدة، والذي جاء باسم درع الخصوصية (Privacy Shield)،[٢] والذي شمل عدة تطورات من أبرزها: أنه تضمن النص على مبادئ تحكم عملية نقل البيانات، منها تقليص البيانات وتحديد أغراض معالجة البيانات، وكذلك منح أصحاب البيانات وسيلـة للطعـن على نقلهـا،[٣] إلا أن هذه التعديـلات لم تـقِ درع الخصوصية من ذراع الإبطال كذلك.

فـي عام ٢٠١٥، قـام ماكسيميليـان شريمز بتدشـين شكوى أمـام مفوضية حماية البيانات الأيرلندية، مدعيًا أن شركة فيس بوك الأيرلندية تقوم بنقل بياناته الشخصية إلى شركـة فيس بوك الأم في الولايـات المتحدة، وأن هذه البيانات المنقولة غير محمية فـي مواجهـة السلطات العامة فـي الولايات المتحـدة، وهو ما يخل بحقوقـه الأساسية بموجب قانون الاتحاد الأوروبي[٤].

(1) El Khoury A, "The Safe Harbour Is Not a Legitimate Tool Anymore. What Lies in the Future of EU-USA Data Transfers?" (2015) 6 European Journal of Risk Regulation 659

(2) Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance) (OJ L 207 01.08.2016, p. 1, ELI: http://data.europa.eu/eli/dec_impl/2016/1250/oj)

(3) Voss WG, "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting "72 The Business Lawyer 231

(4) (Schrems II) Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems, [2020], para 55.

إلى جوار ذلك، ادعى شريمز أنه لا توجد في سبيل حماية بياناته الشخصية وسائل إنصاف قضائي ملائمة في الولايات المتحدة. وقد طلب شريمز أن تقوم المفوضية الأيرلندية بوقف عمليات نقل البيانات تلك[١]، إلا أن المفوضية رأت أنه ينبغي النظر كذلك في البنود التعاقدية القياسية لكونها معيبة، وبالتالي واجبة الإبطال – وذلك باعتبارها الأساس القانوني الساري آنذاك لنقل البيانات من الاتحاد الأوروبي إلى الولايات المتحدة بعد إبطال الملاذ الآمن.

بناءً على ذلك، قامت مفوضية حماية البيانات الأيرلندية بتحريك دعوى أمام المحكمة العليا الأيرلندية، والتي قامت بدورها بإحالة القضية لمحكمة العدل الأوروبية وذلك على أساس النظر في صحة البنود القياسية الحاكمة لنقل البيانات، وذلك في ٢٠١٦ [٢]. إلا أن الأمور أخذت منحًا آخر بأن كانت الاتفاقية الجديدة (الملاذ الآمن) المنظمة لنقل البيانات من الاتحاد الأوروبي إلى الولايات المتحدة قد خرجت إلى النور في العام ذاته. وعلى ذلك مدت محكمة العدل بحثها –المنصب على صحة الأساس القانوني لنقل البيانات – إلى اتفاقية الملاذ الآمن كذلك. ذلك البحث الذي انتهى بحكمها في ٢٠٢٠ ببطلان اتفاقية الملاذ الآمن، وصحة البنود القياسية مع عدم كفايتها في ذاتها لنقل البيانات.

ثانيًا- تحليل الحكم:

قامت محكمة العدل الأوروبية بالبت في الأسئلة المحالة إليها من المحكمة العليا الأيرلندية على الترتيب التالي:

١- استثناءات اللائحة العامة لحماية البيانات الشخصية:

كان فحوى السؤال الأول الوقوف على مدى انطباق اللائحة العامة لحماية البيانات على عملية نقل البيانات التي تتم بين شركتي فيس بوك أيرلندا وفيس بوك الأم

(١) حكم الإحالة من المحكمة العليا الأيرلندية إلى محكمة العدل الأوروبية، الفقرتان ١٧، ١٨، [https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31058]، الزيارة الأخيرة ٢٠٢١/١١/٣٠م.

(٢) حكم الإحالة، فقرة ٤٦.

فـي الولايات المتحدة،[١] باعتبـار أن مصدر التهديد الذي قد تتعرض له البيانات هو تدخـلات سلطـات الأمن القومي في الولايـات المتحدة، ودافعها في ذلـك هو أغراض الأمن القومي. لذا فهو مبحث يتوقف عليه تحديد القانون واجب التطبيق على القضية، وبعبارة أخرى ما إذا كانت اللائحة العامة لحماية البيانات واجبة التطبيق أم لا.

قـدرت محكمة العـدل الأوروبية أن المسألـة القانونية هنا هي مـا إذا كانت اللائحة العامـة لحماية البيانات تنطبق على حالة نقل البيانات الشخصية لأغراض تجارية من إحـدى الدول الأعضاء إلى كيان اقتصادي فـي دولة أخرى، مع تدخل السلطات العامة في عملية المعالجة تلك لأغراض حماية الأمن القومي.

ذلـك السؤال يقصد بـه إذا كانت عملية المعالجة تلك تدخل بـين استثناءات تطبيق اللائحـة المنصوص عليها في المـادة (٢) منها. تلـك الاستثناءات علـى نطاق تطبيق اللائحة تشمل معالجة البيانات الشخصية في سياق نشاط يقع خارج الاتحاد الأوروبي. ومـن الجدير بالذكر هنا أن عمليـة جمع البيانات وتخزينها ونقلهـا هو مما يدخل في معنـى معالجة البيانات، وهو مـا تقوم به شركة فيس بوك أيرلنـدا، لذا فهي لا تخضع لهذا الاستثناء. تشمل الاستثناءات كذلك بعض مسائل السياسة والدفاع الخارجي التي نصـ عليها الفصل الخامس من الباب الخامس مـن اتفاقية تأسيس الاتحاد الأوروبي، وهـو كذلك لا ينطبق على الوضع الحالي. تتضمن الاستثنـاءات أيضًا معالجة البيانات لأغراض شخصية بواسطة أشخاص طبيعيين، والمعالجة لأغراض جنائية.

جـاء إذن جواب المحكمة بالنفي، إذ اعتبرت أن نقل البيانات من فيس بوك أيرلندا إلى فيـس بوك الولايات المتحدة هو عميلة نقل بيانـات إلى خارج الاتحاد الأوروبي، بين كيانـين اقتصاديين، لأغراض تجارية، تتم بواسطـة إلكترونية. وهو ما يعني أنها ليست بواسطـة شخـص طبيعي لأغراض شخصية بحتـة، ولا هي بمناسبـة تحقيق جنائي، وبالكليـة ليـس مما تشملـه الاستثناءات فـي المـادة (٢)[٢]. وحقيقة أنـه تتم معالجة البيانات بواسطة السلطات العامة لأغراض الأمن القومي لا يجنبها تطبيق اللائحة[٣].

---

(١) وقـد ثـار جدل بخصوص معنى «النقل الدولي» حيث لم يرد له ذكر في اللائحة العامـة لحماية البيانات، وكذلك كان الحال توجيـه حمايـة البيانات ١٩٩٥ السابق على اللائحـة. ويشار في هذا الصدد إلى الحكم الصـادر عن محكمة العدل الأوروبية فـي قضيـة Bodil Lindqvist حيث أشارت المحكمة إلى عملية نقـل البيانات على أنها ليست مجرد رفع أو إتاحة المحتوى على للإنترنـت، وإنمـا هي عملية إيجابية تنطوي على نقل البيانات إلى دولة أخـرى، CJEU, Bodil Lindqvist, C-101/01, 6 November 2003

(2) Schrems II, para 85.

(3) Ibid, para 87.

٢- معايير نقل البيانات بواسطة البنود التعاقدية القياسية:

السؤال الثاني يدور حول مستوى الحماية الذي يعد ملائمًا تحت اللائحة العامة لحماية البيانات، وبتعبير المحكمة «العوامل» التي ينبغي أخذها في الاعتبار، عند نقل البيانات للخارج تحت غطاء البنود التعاقدية القياسية.

تناولت المحكمة هذه المسألة بأن أبرزت موقع البنود التعاقدية القياسية بالنسبة لقرار الكفاية، باعتباره آلية احتياطية.[١] أقرت المحكمة أنه في حالة عدم وجود قرار كفاية، تنطبق المادة (٤٦) التي تتيح للمتحكم أو المعالج نقل البيانات للخارج، إذا تمكنوا من توفير ضمانات ملائمة لحمايتها. ووفق هذه المادة، تعتبر البنود التعاقدية القياسية إحدى وسائل توفير هذه الضمانات. وعلى أي حال يجب أن تقرن البنود القياسية أو غيرها من الضمانات – مثل قواعد الشركات الإلزامية – بحقوق قابلة للإنفاذ لصاحب البيانات، ووسائل إنصاف قانوني.[٢]

الحكم لم يحدد حصرًا الحقوق القابلة للإنفاذ، التي قد يتمتع بها صاحب البيانات، ولم تفعل أيضًا اللائحة العامة لحماية البيانات. لكنه من المفهوم أنها تشتمل على الأقل على الحقوق التي نصت عليها اللائحة لصاحب البيانات في الفصل الثالث. إذ يتمتع صاحب البيانات في حق الوصول للبيانات، والحق في تصحيحها إذا ما وجد فيها خطأ، كما يحق له أن يقيد معالجة البيانات، وأن يمحوها. ينبغي فوق ذلك أن يتم إخطار صاحب البيانات إذا تم جمعها بطريق على غير رضائه وفقًا لما تسمح به المادة (٦)، وله أيضًا أن يعترض على معالجة بياناته في هذه الحالة بما تتيحه المادة (٢١).

هذه الحقوق في تفسيرها وفهمها، تخضع للقراءة في ظل المبادئ التي استحدثتها اللائحة في المادة (٥)، وذلك باعتبار هذه المبادئ بمثابة الغطاء العام والمرجع في فهم حدود وأبعاد معالجة البيانات والالتزامات المرتبطة به مما توقعه اللائحة[٣].

أما فيما يتعلق بوسائل الإنصاف القانوني، فيترتب عليها تمكين صاحب البيانات من تحريك دعوى قضائية إذا ما تراءى له ذلك. ومن المستفاد من هذا الحكم أن توفير

---

(١) وفقًا للحيثية ١٠٨ من اللائحة، في حالة عدم وجود قرار ملاءمة، فإنه الضمانات الملائمة التي يفترض العمل بها لنقل البيانات – والتي تعتبر البنود القياسية إحدى وسائلها– يجب أن «تعوض النقص في حماية البيانات في الدولة الأخرى».

(2) Schrems II (n 1), para 91.

(3) Lee A Bygrave, Data Privacy Law (Oxford University Press 2013), 145.

وسائل الإنصاف القانوني له ضوابط خاصة، وبالتالي فإن هذا الشرط لا يستقيم بمجرد أن يتوافر في الدولة المستضيفة للبيانات مجرد جهة مظلمة، تعمل على استقبال الشكاوى المتعلقة بنقل البيانات.

وقد تضمن منطوق الحكم في هذه النقطة تأكيدًا من المحكمة على فكرة تساوي مستوى حماية البيانات الذي يكفله قانون الاتحاد الأوروبي ومستوى الحماية الذي تأتي به هذه الضمانات. ويمكن أن نستخلص من تأكيد المحكمة في هذا الصدد أن معيار مستوى الحماية المساوي هو حجر الزاوية في أية عملية نقل بيانات للخارج أيًا كانت الوسيلة التي تعتمد عليها، سواء كانت قرار ملاءمة أو غير ذلك. وهذا ليس التناول القضائي الأول لهذه الفكرة، إذ أكد عليها أيضًا حكم المحكمة ذاتها في قضية شريمز ١. ذلك الحكم أرسى لمعيار في غاية الأهمية بأن أوضح أن مستوى الحماية المساوي لا يعني التطابق بين الحماية القانونية للبيانات في الدولة المستقبلة والاتحاد الأوروبي، وإنما يقصد به التساوي في جوهر الحماية. وهو ما يترتب عليه أنه لا يفترض بالضرورة أن يتم اتباع الآليات ذاتها، وأن يحتوي التنظيم القانون على النصوص ذاتها، وإنما يكفي أن تتوافر بدائل في جوهرها متكافئة الحماية.

ارتقت المحكمة بهذا المعيار إلى حد المبدأ بأن قررت أن نقل البيانات عبر البنود القياسية لا يختلف عن نقلها عبر قرار الملاءمة، من حيث إن تلك البنود تفترض أيضًا مستوى حماية مساوٍ في جوهره للمستوى المطبق في الاتحاد الأوروبي[1]. تعميم هذا المعيار هو قراءة صائبة تجد مصدرها في المادة (٤٤) – فاتحة الفصل الخامس– من اللائحة العامة لحماية البيانات التي ترسي المبدأ العام لنقل البيانات إلى الخارج. مفاد هذا المبدأ هو أن يتم تطبيق كل أحكام نقل البيانات، بحيث تضمن أن مستوى الحماية الذي تكفله هذه اللائحة لا يتم تقويضه. واتساقًا مع هذا يأتي معيار مستوى الحماية المساوي، الذي يتطلب بدوره أن يكون هناك من الضمانات لدى الدولة مستقبلة البيانات أو من خلال مستقبل البيانات ذاته ما يضمن توافر مستوى مساوٍ في حالة نقل البيانات للخارج، وبالتالي لا تصبح القيمة التي أتت بها اللائحة مهددة بالإهدار إذا ما نقلت البيانات لخارج الاتحاد الأوروبي.

(1) Ibid, para 96.

علاوة على ذلك، فقد أشار الحكم إلى المناطق التي ينبغي النظر إليها بحثًا عن تحقق معايير قياس مستوى الحماية. وهنالك موطنان للبحث عن الملاءمة، ينبغي بحثهما معًا، ولا يغني أحدهما عن الآخر: بنود العقد بين المتحكم أو المعالج الموجود في الاتحاد ومستقبل البيانات في الدولة الآخر، ذلك من ناحية. من ناحية أخرى، يتوجب النظر إلى الجوانب ذات العلاقة في النظام القانوني للدولة التي ستنقل إليها البيانات[1]. ويتوجب الملاحظة هنا أن تعبير «الجوانب ذات العلاقة في النظام القانوني» تختلف عن مجرد النظر في القوانين، فالأول أشمل من الثاني، ويشمله، ذلك أنه ربما تكون القوانين ذاتها مصونة، إلا أن واقع تطبيقها ليس كذلك، وهو ما يعني سلامة القوانين وفساد النظام القانوني. لذلك لما أشارت اللائحة، ومن ثَمَّ الحكم، كانت الإشارة للجوانب ذات العلاقة في النظام القانوني.

٣- التزام السلطات الرقابية (Advisory Authorities)**:**

كان السؤال الذي نظرته المحكمة هنا هو: هل يتوجب على السلطات الرقابية في دول الاتحاد الأوروبي أن توقف عمليات النقل التي تتم بموجب بنود قياسية معتمدة من قبل المفوضية الأوروبية، إذا ما قدرت أنه لا يتم الامتثال لالتزامات حماية البيانات أو لا يمكن الالتزام بها؟

وهنا يتم التمييز بين تصورين، أحدهما أن يوجد قرار ملاءمة، والآخر ألا يوجد، وأن يكون نقل البيانات بناءً على بنود قياسية مثلًا، وهي الحالة التي كانت مناط التساؤل في قرار الإحالة أصلًا.

ولفهم مناط الاختلاف، ينبغي فهم الفرق بين الحالتين من حيث المبدأ، وهو أن قرار الملاءمة يكون صادرًا من المفوضية الأوروبية، وهي مؤسسة تابعة للاتحاد، وبالتالي لا يحق للمؤسسات الوطنية –متمثلة في السلطات الإشرافية – تجاوزها. وقرار الإحالة ذاته يكون بمثابة إقرار بملاءمة النظام القانوني للدولة المنقول إليها البيانات ككل، بما يشمل التنظيم القانوني والممارسات الجارية في الدولة المستقبلة. أي أنه يعتبر مظلة ضمان عامة. وللوصول إلى تلك المرحلة يتطلب من المفوضية أن تجري اختبار ثلاثي الأجزاء يشمل سيادة القانون، ووجود سلطات إشرافية فعالة، والالتزامات الدولية

(1) Ibid.

للدولة مستقبلة البيانات، مما يوضح مدى اتساع قاعدة التحوط الذي يبنى عليها قرار الكفاية. ولذلك مجرد صدور قرار كفاية يغني عن الحاجة لأي تصريح لاحق لنقل البيانات إلى الدولة التي حازت هذا القرار.

بينما -على الكفة الأخرى- البنود التعاقدية القياسية، هي مجرد نماذج لبنود تعاقدية يمكن للمؤسسات التي تعتزم نقل البيانات للخارج تضمينها في عقودها مع الأطراف المستقبلة للبيانات من خارج الاتحاد. يقوم بوضعها أيضًا المفوضية الأوروبية، أو السلطة الإشرافية للدولة، إلا أن مسئولية تطبيقها تقع على المؤسسات مرسلة البيانات دون ضمان مقدم بأنه سيتم الامتثال لها أو أن لتلك المؤسسات القدرة على إنفاذها. لذلك فهي تخضع لرقابة السلطات الإشرافية.

وأما بالنسبة للحالة اللاحقة، عند نقل البيانات وفقًا للبنود القياسية، فإن السلطات الإشرافية «مطالبة» بأن توقف أو تحظر نقل البيانات إلى الدولة الأخرى حال لم يتم الامتثال، أو لم يكن من الممكن الامتثال للبنود القياسية التي يتم نقل البيانات على أساسها[١]. ويضيف الحكم أنه حتى في حالة وجود قرار ملاءمة، فإن ذلك لا يمنع السلطات الإشرافية من النظر في الشكاوى المقدمة إليها بخصوص حماية البيانات في هذا الصدد. وبالرغم من أنها لا تملك في مثل هذه الحالات أن توقف نقل البيانات أو تحظره، إلا أن لها على ما يتبدى لها من مخالفات أن تحرك دعوى أمام القضاء الوطني، الذي قد يحيل بدوره الأمر لمحكمة العدل الأوروبية للقرار في صحة قرار الملاءمة من عدمها[٢].

٤- مدى صحة البنود التعاقدية القياسية (قرار المفوضية رقم ٢٢٩٧ لسنة ٢٠١٦):

بحثت المحكمة السؤال حول مدى قدرة البنود التعاقدية القياسية (ذاتها) على توفير مستوى حماية كاف، بالرغم من أنها غير ملزمة للسلطات الإشرافية في الدول التي يتم نقل البيانات إليها خارج الاتحاد الأوروبي.

وقت أن حرك ماكس شريمز الدعوى الحالية لم تكن اتفاقية درع الخصوصية قد

(1) Ibid, para 121.
(2) Ibid, para 120.

خرجت للضوء بعد، وكان مطعنه آنذاك متمثلًا في أن نقل البيانات إلى الولايات المتحدة الأمريكية غير ضروري ويقوض سلامة هذه البيانات. تمثل الخطر الأكبر على البيانات في برامج الاستخبارات التي تطبقها أجهزة الاستخبارات والأمن القومي الأمريكية تحت مظلة القانون الأمريكي، والتي تتيح لها الولوج وجمع البيانات الشخصية الواردة من الاتحاد الأوروبي بما لا يتفق ومستوى الحماية الذي يتيحه قانون الاتحاد الأوروبي. وفي غياب قرار ملاءمة – لعدم اعتماد الاتفاقية بعد – كان نقل البيانات يتم وفقًا للبنود القياسية. ولذلك كان من المنطقي أن يثور التساؤل حول ما إذا كانت الالتزامات الناشئة عن هذه البنود تنصرف إلى السلطات العامة في الدولة مستقبلة البيانات، ومدى صحة البنود التعاقدية القياسية إذا كانت غير ملزمة لهذه السلطات. وحيث إن قرار الكفاية (درع الخصوصية) قد صدر أثناء نظر محكمة العدل الأوروبية للدعوى، فقد مدت قضاءها ليشمل القرار إلى جانب البنود التعاقدية القياسية السارية آنذاك. وبالتالي أصبحت الوسيلتان الأكثر شيوعًا لنقل البيانات إلى خارج الاتحاد الأوروبي محل بحث المحكمة، وصارت حركة البيانات من الاتحاد الأوروبي إلى الولايات المتحدة مهددة بشدة. وفي السؤال الرابع تعرضت المحكمة أولًا إلى الوسيلة الأسبق: البنود التعاقدية القياسية.

سلمت المحكمة أولًا بأنه من المتفق عليه أن البنود القياسية تلزم فقط أطراف التعاقد، أي المتحكم أو المعالج الناقل للبيانات والطرف الآخر مستقبل البيانات في الدولة الأخرى، وذلك دون أن يكون لها أي قوة إلزامية في مواجهة السلطات العامة في هذه الدولة، إذ إنها أداة ذات طبيعة تعاقدية خالصة[1].

بناءً على تلك النتيجة، استأنفت المحكمة بحثها بالتمييز بين صحة البنود القياسية في ذاتها، والتوافر الفعلي للضمانات الملائمة. ذلك كي تتمكن فيما بعد من تحديد موقفها من صحة البنود القياسية.

يتضح من قراءة الحكم أن مجرد صحة البنود القياسية لا يكفي في ذاته للقطع بتوافر ضمانات ملائمة لحماية البيانات وفقًا لما تقتضيه المادة (١/٤٦) من اللائحة. فالبرغم من أن مستقبِل البيانات من خارج الاتحاد الأوروبي قد يتعهد بموجب البنود

(1) Ibid, paras 125, 130.

القياسية بأن يقوم باتخاذ التدابير التي تحقق الحماية نظريًّا، إلا أنه عملًا قد لا يسمح الواقع القانوني أو قوانين البلد مستقبلة البيانات بأن يوفي بالتزاماته بحماية البيانات، خاصةً إذا ما كان القانون يخول السلطات العامة التدخل في البيانات.

والمستفاد من ذلك أن صحة نقل البيانات وفقًا للبنود القياسية – وهنا نقول صحة نقل البيانات وليس صحة البنود القياسية – يتوقف على عاملين معًا، أولهما صحة البنود ذاتها، وثانيهما الواقع القانوني في الدولة المنقول إليها البيانات وقدرة مستقبل البيانات على تطبيق هذه البنود في ضوء ذلك الواقع القانوني[1]. وتلك نتيجة منطقية لما أوضحناه من طبيعة البنود القياسية؛ حيث إن صحة البنود ذاتها مطلب بطبيعته سابق على صحة تطبيقها على الواقع العملي، وبحث ما قد تصطدم به من عقبات.

يؤكد الحكم على الفرق بين البنود القياسية وقرارات الكفاية، فيؤكد على أن المقارنة تصب في صالح الأخير حيث إن إصدار قرار الكفاية يتطلب من المفوضية الأوروبية أن تتأكد مما إذا كانت القوانين ذات الصلة بحماية الأمن القومي في الدولة مستقبلة البيانات تكفل مستوى كافٍ من الحماية، وأن نقل البيانات إلى دول أخرى لا يتأثر باتصال سلطات الأمن القومي بها. أما فيما يتعلق بالبنود القياسية، فإن المادة (٤٦/١) لا يمكن أن يستدل من نصها على أن المفوضية مطالبة بأن تفحص مستوى الحماية الذي تكفله الدول. وبعبارة أخرى، فإن مستوى الحماية الذي تكفله الدولة ذاتها ليس من شأن البنود التعاقدية القياسية، فالبنود القياسية هي بنود توضع كنموذج بشكل موحد بصرف النظر عن المؤسسات والشركات التي ستنطبق عليها أو الدول التابعة لها. لذلك فإنها مسئولية المتحكم أو المعالج أن يتأكد من أن مستوى الحماية في الدولة مستقبلة البيانات كافٍ أم لا، آخذًا في الاعتبار التنظيم القانوني فيها إذا ما طُبقت في ظله البنود التعاقدية. ويصير لزامًا عليه إذا ما اتضح له عدم الملاءمة أن يوقف أو ينهي عملية نقل البيانات.

في ضوء ذلك، كان استنتاج المحكمة أن عدم إلزامية البنود التعاقدية القياسية للسلطات العامة في الدولة مستقبلة البيانات غير مؤثر على صحة هذه البنود.

(1) Ibid, para 126.

أمـا بالنسبة للسؤال الآخر، وهو ماهية العوامـل المؤثرة على صحة البنود القياسية، قـدرت المحكمة أنه من العوامل المؤثرة على صحة البنود القياسية هو ما إذا كانت توفر من الآليات ما يكفل حماية للبيانات وفقًا لما يقتضيه قانون الاتحاد الأوروبي، ومن ناحية أخرى أن يضمن أنه في حالة استحالة الامتثال لمقتضيات الحماية تلك أو انتهاكها، أن يتم وقف أو إنهاء نقل البيانات.

وببحـث البنود نجـد أن هذه العناصر قد توافرت – على مـا رأت المحكمة. ذلك أن البنـد ٥/أ علـى سبيل المثال يوقع التزامًا على مستقبل البيانـات بإخبار المتحكم إذا ما طـرئ طارئ يحول بينه وبين التزاماته. كما أن مستقبل البيانات يقر بموجب هذا البند بـأن قانـون دولته لا يعـوق امتثاله بالتزاماتـه الناتجة عن العقد. وهو يتعهـد أيضًا بأن يخطـر المتحكم أو المعالـج مرسل البيانات إذا جد ما يخالف ذلـك. كما تم النص على حق المتحكم أو المعالج في إنهاء التعاقد في حالة عدم امتثال مستقبل البيانات أو عدم قدرته على الامتثال.

لذلـك انتهت المحكمة إلى الحكم بأن البنـود التعاقدية القياسية فعالة، استنادًا إلى أنهـا تترك عبء تقديـر الملاءمة على المتحكم أو المعالج المرسلـين للبيانات إلى الخارج بحيث تصبح المسئولية موقعة عليهم.

إذن فالنتيجـة النهائيـة أن البنود القياسية فـي ذاتها سليمة وتوفـر وسائل حماية فعالـة. وذلك استنتاج صحيح من جانب المحكمـة، إذ إن المسألة المبحوثة هنا تنصرف إلى صحة قرار المفوضية الأوروبية باعتماد البنود التعاقدية القياسية في العموم وبشكل نظـري. ويترتب على ذلك أن يصبح مدى صحة تطبيق هذه البنود على أرض الواقع هو مسألـة أخـرى، تنطبق على أساس فردي في كل حالة على حدة. وهو ما يغدو معه بحث صحـة تطبيق البنود القياسية إذا ما اعتمدتها شركتـا فيس بوك أيرلندا وشركة فيس بـوك الأم –باعتبار الأولى المتحكم في البيانات والثانية مستقبل البيانات في الخارج– هـو مسألـة خارجة عن نطاق هذه القضيـة ومتروك أمرها في المقـام الأول للمفوضية الأوروبية وكذلك للسلطة الإشرافية المعنية. ذلك إن أكد على شيء فهو يؤكد مرةً أخرى علـى أن دور المتحكم أو المعالج الذي يقوم بنقـل البيانات يتعاظم تحت البنود القياسية حيـث ينبغي عليه أن يتأكد من صحة النظام القانوني، وفي المجمل من ملاءمة مستوى

الحمايـة. فـإذا تبين له عدم الملاءمة، توجب عليه أن يتخذ تدابير إضافية للوصول إلى المستوى الملائم،[1] وإذا تعذر ذلك كانت النتيجة الحتمية هي وقف نقل البيانات.

٥- صحة درع الخصوصية:

رأت المحكمـة أن الإجابة على جوهر الشكوى الأصلي، هـو أن نقل البيانات للولايات المتحـدة لا يكفل مستوى ملائمًا من الحماية، يتطلب بحث صحة قرار درع الخصوصية الصـادر من المفوضيـة الأوروبية باعتباره الأساس القانـوني لنقل البيانات بين الاتحاد الأوروبي ومنظمات الولايات المتحدة آنذاك، حتى وإن كان قد صدر عقب تقديم الشكوى.

مـن الجدير بالذكر أن أحد المآخذ الرئيسية على القانون الأمريكي من حيث مستوى الحمايـة هـو القوانين المنظمـة لنشاط الاستخبـارات، وما تتيحه مـن سلطات قد تمثل انتهـاكًا للقانون الأوروبي. على رأس هذه القوانـين قانون مراقبة الاستخبارات الأجنبية (Intelligence Surveillance Act (FISA، وتحديدًا المادة (٧٠٢) التي تسمح بالاستخبار الإلكـتروني ضـد غـير الأمريكيين خـارج الولايات المتحدة، مـع إمكانية إجبـار مزودي الخدمة الإلكترونية -مثل مواقع التواصل الاجتماعي- على إتاحة البيانات اللازمة. يتم تطبيق هذه المادة من خلال برامج استخباراتية مثل UPSTREAM وPRISM.

بالإضافـة إلى ذلك فإن الرئيس الأمريكي باستطاعتـه توجيه أنشطة الاستخبارات الأمريكية بموجـب أداتين هما الأمر التنفيـذي ١٢٣٣٣ (Executive Order ١٢٣٣٣)، وتوجيـه السياسـة الرئاسيـة (Presidential Policy Directive ٢٨ (PPD-٢٨). إذ يهـدف الأول إلى منح وكالـة الاستخبارات الأمريكية ومجتمـع الاستخبارات الأمريكي القـدرة على جمـع البيانات لأغراض الاستخبارات ومكافحة الاستخبـارات الأجنبية، وألـزم الأجهـزة الفيدرالية بالتعاون معها فـي إعطاء البيانات اللازمـة. بينما الثاني يهدف إلى تقنين وإخضاع عمليات الاستخبارات إلى اعتبارات حقوق الإنسان.

السمو:

تناولـت المحكمة أولًا القيد العام الواقع على كافة ضمانات درع الخصوصية. يحتوي درع الخصوصية على قيد على كامل القرار (درع الخصوصية) في الملحق ٢، فقرة ١/٥

(1) Ibid, para 133.

مفـاده أنه يمكن تعطيـل كافة المبادئ التي يتبناها القرار إذا ما تطلبت اعتبارات الأمن القومي، أو المصلحة العامة أو إنفاذ القانون في الولايات المتحدة ذلك. هذا المأخذ ليس بالجديـد، إذ تناولتـه محكمة العدل الأوروبية في حكمها فـي شريمز ١ أيضًا.[١] وكان تفسير المحكمة أن هـذا الاستثناء شديد العمومية، يضع القانون الأمريكي والاعتبارات الأمريكية في مرتبة أعلى من قانون الاتحاد الأوروبي. ذلك التفسير قد تأكد مرة أخرى من خلال منطوق المحكمة في القضية الحالية، إذ أخذت هذا القيد – الذي تكرر في درع الخصوصيـة – على أنه يعني سمو المصلحة الأمريكية على الحقوق الأساسية لأصحاب البيانات، وعلى رأسها الحق في الخصوصية وحماية البيانات الشخصية. وأبرز مثالبه هو أنه يضع قيدًا على كل الضمانات، وهو قيد غير محدود، ليس له ضوابط كافية.

برامج الاستخبارات:

تناولـت المحكمـة بالبحـث، فيما تلـى، مسألة كفاية مستـوى الحماية فـي القانون الأمريكـي. وفي سبيـل ذلك أسسـت لحكمها بالإشـارة إلى ميثاق الحقـوق الأساسية للاتحـاد الأوروبي، تحديدًا المادة (٢/٨)، والتـي تستهدف حماية البيانات الشخصية. تقتضـي المـادة (٨) أن يكون نقل البيانـات بطريقة عادلة، لأغراض معينة، وأن يكون ذلـك برضاء صاحـب البيانات. في حالة توقيع قيد على هذا الحـق، فإنه يتوجب، كما تحتم المادة (١/٥٢)، أن يكون ذلك وفقًا لتنظيم قانوني يحدد حدود ونطاق هذا القيد. تضيـف المحكمـة على مضمون المـادة (٥٢) في هذا الصدد أن يكـون سند القيد ذاته محـددًا لنطاقه وأثـره على الحقوق ذات الصلـة. بالإضافة إلى ذلـك ينبغي كذلك أن يخضـع ذلـك القيد لمبدأ التناسب، والـذي يقتضي بدوره أن تكون هنـاك ضرورة تدفع لتقييـد الحـق[٢]. هذه الضوابط تمثـل تجسيدًا للاختبار ثلاثي الخطـوات الراسخ في قضـاء محكمة حقوق الإنسان الأوروبية، والذي يجـد أساسه في العهد الدولي للحقوق المدنيـة والسياسيـة. وفقًا للأخـير يتوجب للقيد على الحـق أو الحريـة أن يكون القيد موصوفًـا في القانون، وأن يستهدف خدمة غرض مشروع، وأن يكون ضروريًّا ومتناسبًا في مجتمع ديمقراطي. إذا ما تخلف القيد عن أيٍ من هذه الضوابط، يضحى باطلًا.

وبتطبيق ذلك على برامج الاستخبارات، نجد أن المادة (٧٠٢) من قانون المراقبة وإن

(1) Schrems I, para 186.
(2) Schrems II, para 174.

كانت تخضع عمليات المراقبة لمحكمة أنشئت لهذا الغرض، إلا أن رقابة المحكمة تقتصر على التأكد من أن البرنامج برمته يتعلق بهدف الحصول على معلومات استخباراتية أجنبية. لكن رقابة هذه المحكمة تقف قاصرة عن التأكد مما إذا كان تطبيق هذه البرامج على الحالات الفردية بهدف الحصول على المعلومات الاستخباراتية صحيحًا أم لا. ذلك بجانب أن المادة لا تنطوي على ضمانات لأصحاب البيانات من غير الأمريكيين، والذين يمكن استهدافهم بهذه البرامج[1]. ذلك يخل بالمتطلبات سالفة الذكر، فالقيد الذي توقعه برامج الاستخبارات سالفة الذكر بموجب المادة (٧٠٢) من قانون المراقبة عجز عن تأطير نطاق القيد على الحق في حماية البيانات الشخصية، وإنما أطلق يد السلطات المعنية في تقدير ذلك، مما يخل بمبدأ التناسب على ما أشرنا. إذ يتطلب الأخير أن يكون هناك أساس قانوني يتم بناءً عليه تقييد للحقوق الأساسية للأفراد، وأن يحدد ذلك السند القانوني ذاته نطاق القيد على الحق، وأن يحدد بشكل واضح ومحدد المعايير التي تحكم نطاق وتطبيق الإجراء المقيد للحرية، وأن تكفل فوق ذلك كله حدًا أدنى من الضمانات ضد التعسف.

وبالرغم من أن توجيه السياسة الرئاسية ٢٨ ينص على مبادئ تحكم عمليات الاستخبارات القائمة على نقل الإشارات، وتهدف إلى حماية حقوق أصحاب البيانات، إلا أن هذه المبادئ لم تقر حقوقًا بعينها لأصحاب البيانات يمكنهم اتخاذها أساسًا للملاحقة القضائية أمام المحاكم. وهو ما يخل إذن بقاعدة مستوى الحماية المساوي، حيث يفترض وفقًا للمادة (٤٥/٢/أ) من اللائحة أن يتمتع صاحب البيانات بحقوق قابلة للإنفاذ القضائي. بالإضافة إلى ذلك، فإنه يسمح بجمع كميات ضخمة من البيانات إذا تعذر التعرف أو الوقوف على مصدر خطر الاستخباراتي تحديدًا. يسمح ذلك للبرامج المبنية على الأمر التنفيذي ١٢٣٣٣ أن تلج إلى البيانات التي تمر عبر الولايات المتحدة الأمريكية، دون أن تخضع عملية جمع البيانات تلك لأي رقابة قضائية. ذلك النطاق الفضفاض لجمع البيانات عبر الأمر التنفيذي ١٢٣٣٣ دون رادع من التوجيه ٢٨، يخل بمبدأ التناسب، وبالتأكيد ينال من مبدأ الضرورة. لذلك رأت المحكمة أن برامج الاستخبارات المعتمدة على هذا الأمر التنفيذي لا توفر هي الأخرى حقوقًا قابلة للإنفاذ القضائي.

(1) Ibid, para 180.

الحق في اللجوء للقضاء:

على صعيد آخر، تقتضي قاعدة مستوى الحماية المساوي – بحسب المادة (٤٥/٢/أ) – أن تكـون هناك وسائل إنصاف قضائي فعالة لأصحاب البيانات. أي بعبارة أخرى أن يكـون لهـم الحق في اللجوء للقضـاء للتظلم من التعامل في بياناتهـم الشخصية. من تبعات قضية شريمز ١ هو استحداث درع الخصوصية لمنصب محقق الشكاوى والخاص بغرض فحص الشكاوى (Privacy Shield Ombudsperson) التي يتقدم بها أصحاب البيانات. ودوره في النظام الأمريكي هو «منسق لدبلوماسية تكنولوجيا المعلومات».

بالنظر إلى أن مطلب وسائل الإنصاف القضائي يحتم أن تكون هناك محكمة مستقلة ونزيهـة، فـإن آلية محقق الشكاوى تعجـز عن توفية المطلب، حيـث إن محقق الشكاوى يعتمـد في القيام بمهامه علـى وزير الخارجية. فهو يفترض به أن يقوم بتقديم تقاريره مباشـرةً لوزير الخارجيـة الذي يعمل على إزالـة العوائق والتأثـير الخارجي على عمل محقـق الشكاوى. وفـوق ذلك فإن محقق الشكاوى يتم تعيينه مـن قبل وزير الخارجية، ويعتبر كذلك تابعًا لوزارة الخارجية، وذلك دون أن توجد ضمانات خاصة بعملية تعيينه أو عزلـه بما يكفل استقلاله عـن السلطة التنفيذية. وبالإضافـة إلى الأسباب السابقة التـي تحول دون اعتبار آلية محقق الشكاوى وسيلة إنصاف قضائي ملائمة، فإن القائم بهـذا الدور لا يملك أن يصدر قرارات ملزمة لجهات الاستخبارات المعنية. وبأخذ ذلك بعـين الاعتبار يتبـدى أن آلية محقق الشكاوى فشلت في توفير مستوى حماية مساوٍ في جوهره لنظيره في الاتحاد الأوروبي، ذلك أن المادة (٤٧) من ميثاق الحقوق الأساسية للاتحـاد الأوروبي تمنـح الحق في الحصول على وسائل إنصـاف قضائي فعالة والحق في محاكمة عادلة، الأمر الذي يتعذر على محقق الشكاوى أن يقوم به.

ثالثًا- التعقيب على الحكم:

لقـد جذب هذا الحكـم أنظار المهتمـين بحماية البيانـات في جميع أنحـاء العالم، ليـس فقط لأن الاتحـاد الأوروبي يشغل موقع الريادة في مجـال تنظيم حماية البيانات الشخصيـة، ممـا يجعل قـرار محكمة العدل الأوروبيـة مرجعًا مهمًا لـكل العاملين في المجال، وإنما أيضًا لأنه وضع اتفاقية درع الخصوصية موضع تهديد، وهي التي لم تظهر إلى الضوء إلا لأن سابقتها «الملاذ الآمن» قد طالها الإبطال أيضًا من المحكمة ذاتها في

وقت ليس ببعيد. ذلك أضفى أهمية خاصة على ذلك الحكم؛ لأنه يعد محاولة أخرى لفهم أدق لحدود حماية البيانات الشخصية تحت قانون الاتحاد الأوروبي.

وبالفعل فإن الحكم قد أسهم في إزالة الغبار عن بعض القواعد والمفاهيم الحاكمة لحماية البيانات في القانون الأوروبي. لقد صادف الحكم الصواب بأن أكد على مبدأ مستوى الحماية المساوي، ورسخ أن التساوي في مستوى الحماية في الدولة مستقبلة البيانات والاتحاد الأوروبي هو سمة عامة، ومعيار رئيسي تتقيد به أي عملية نقل بيانات لخارج الاتحاد الأوروبي، أيًا كان الغطاء القانوني لعملية النقل. لذا فإن نقل البيانات عبر قرار الكفاية وفقًا للمادة (٤٥) من اللائحة العامة لحماية البيانات يلزم معه التحقق من توافر «مستوى حماية مكافئ». ليس هذا فحسب، ففي حالة الاعتماد على البنود التعاقدية القياسية أو غيرها من الوسائل البديلة التي توفر ضمانات ملائمة وفق المادة (٤٦)، فإنها يجب أن تقرأ في ظل المادة (٤٤) التي تتطلب ألا تخل عملية النقل بمستوى الحماية الذي تكفله هذه اللائحة[١]. ولما كانت هذه المادة بمثابة الشريعة العامة لكل عمليات النقل، فإن مبدأ مستوى الحماية المساوي الذي تتضمنه يصير واجب التطبيق على كل عمليات النقل كذلك.

وبالرغم من أن هذه المسألة لم تكن محل تناول بعض من قاموا بتحليل الحكم من قبل،[٢] إلا أنها تعتبر من المسائل المهمة؛ لأنها ببساطة ترسي القواعد التي ينبغي على كل المعنيين بمجال حماية البيانات في الاتحاد الأوروبي، والمتعاملين في بيانات الاتحاد الأوروبي من الدول الأخرى، النظر إليها عند تقدير ما إذا كانت ضمانات نقل البيانات المتوفرة كافية أم لا، وبالتالي ما إذا كانت عمليات النقل ذاتها صحيحة أم لا. وذلك يشمل الكيانات المصدرة للبيانات، وكذلك الكيانات المستقبلة، والسلطات الإشرافية في دول الاتحاد الأوروبي المختلفة.

من الجدير بالملاحظة في هذا الشأن أن ما يتم النظر إليه لتحديد انطباق معيار مستوى الحماية المساوي يختلف باختلاف الوسيلة القانونية لنقل البيانات مما أتى به الباب الخامس من اللائحة العامة لحماية البيانات. فنطاق البحث بالنسبة لقرارات الملاءمة ينصرف إلى الجوانب القانونية والعملية المرتبطة بحماية البيانات في الدولة

(1) Ibid, para 92.
(2) Zalnieriute M, "Data Transfers After Schrems II: The EU-US Disagreements over Data Privacy and National Security" 55 Vanderbilt Journal of Transnational Law

مستقبلة البيانات. أما إذا تعلق الأمر بالبنود القياسية، فمسئولية التطبيق العملي للمعايير التي تأتي بها البنود تقع على مصدر البيانات. ما يجب على المفوضية الأوروبية أو السلطة الإشرافية عند صياغتها هو التأكد من وضع ضمانات عقدية إذا التزم بها المتحكم أو المعالج مصدر البيانات – ومن ناحية أخرى مستقبل البيانات – يتحقق مستوى حماية مساوٍ.

من الاستنتاجات الواجبة في هذا الصدد أيضًا هو أن مستوى الحماية هو مرآة للتطورات في قانون حماية البيانات الشخصية في الاتحاد الأوروبي –أي أنه معيار متغير وليس ثابتًا – فهو يخضع لتغير القاعدة القانونية الحاكمة لحماية البيانات الشخصية والخصوصية في الاتحاد الأوروبي، بما في ذلك التحديثات في اللائحة العامة لحماية البيانات، وإصدارات مجلس حماية البيانات الأوروبي، وأحكام محكمة العدل الأوروبية، وغيره مما يسهم في تشكيل هذه القاعدة. وفي ضوء ذلك كله، يتضح مدى قانونية عملية النقل يعتمد على مستوى الحماية في الاتحاد الأوروبي ذاته، والذي يخضع للتغير بتغير قوانين حماية البيانات هناك. كما تتأثر أيضًا بوجه العملة الآخر متمثلًا في مستوى الحماية في الدولة الأخرى، وما يكفله مستقبل البيانات من ضمانات، وهو بدوره قابل للتغير عن طريق تغيير التنظيم القانون لحماية البيانات سواءً بزيادة الضمانات والحماية أو تخفيضهم.

نرى أيضًا أن المحكمة قد أصابت حينما أكدت على التفسير الذي أنزلته من قبل على المادة (٤٥) في قضية شريمز ١. إذ أوضحت أن المادة (٤٥) من اللائحة عندما تطلبت مستوى حماية ملائمًا في الدولة التي ستنقل لها البيانات، فإن ذلك لم يكن يعني أن يكون مطابقًا لمستوى الحماية في الاتحاد الأوروبي. وإنما يجب فهمه على أنه يكفل حمايةً للحقوق والحريات الأساسية متناسبةً في جوهرها مع ما يقدمه قانون الاتحاد الأوروبي من حماية[١]. وعلى سبيل التحديد، فإن العوامل التي ينبغي النظر إليها لتقييم ذلك هي توافر ضمانات ملائمة، وحقوق قابلة للإنفاذ، وسبل إنصاف قانوني فعالة[٢].

أصابت المحكمة كذلك بأن أبرزت عجز النظام الأمريكي عن توفير سبل إنصاف

(1) Schrems II, para 94.
(2) Ibid, para 105.

قانوني فعالة لأصحاب البيانات المنقولة من الاتحاد الأوروبي باعتباره مطلبًا أساسيًا لتوفير مستوى حماية مساوٍ. فالتعديل الرابع من الدستور الأمريكي لا يكفل للمواطنين الأوروبيين حماية الخصوصية التي يوفرها للمواطنين الأمريكيين، وكذلك هو الأمر بالنسبة لقانون مراقبة الاستخبارات الأجنبية.

ولا يغني عن ذلك ما أتت به الاتفاقية من إنشاء نظام متلقي الشكاوى، لأنه يتبع وزارة الخارجية الأمريكية، كما أن القائم بهذا الدور لا يملك سلطة إجبار أي من سلطات الدولة على ما يتوصل إليه من نتائج. ذلك الموقف من المحكمة تترتب عليه نتيجة مهمة مفادها أن مطلب «سبل الإنصاف القانوني» هو مطلب ذو سمات خاصة، لا يقيمها مجرد توفير جهة لتلقي الشكاوى من أصحاب البيانات. ذلك المطلب لابد من قراءته وفهمه في ظل اللائحة وميثاق الحقوق الأساسية للاتحاد الأوروبي. فالمادة (٣٥/٢/أ) تتطلب لإصدار قرار ملاءمة أن تكون هناك وسائل إنصاف قضائي وإداري لأصحاب البيانات. ذلك يعني أن تكون هناك جهة ذات اختصاص قضائي يكون لها سلطة الفصل في شكاوى انتهاك حقوق أصحاب البيانات بشكل ملزم. تتطلب المادة كذلك وجود سلطة إشرافية تعنى بشئون حماية البيانات الشخصية. هذه السلطة الإشرافية يفترض بها أن تكون مستقلة وفعالة، وأن يكون في حوزتها وسائل إنفاذ ملائمة، ويفترض بها أن تخضع للرقابة القضائية في قراراتها[١]. شرط إتاحة اللجوء القضائي إذن هو شرط جوهري، أشارت له اللائحة بالنسبة لمعالجة البيانات داخل الاتحاد الأوروبي، والأمر سواء بالنسبة للدولة مستقبلة البيانات كذلك. هو أيضًا تطبيق جوهري لما تفرضه المادة (٤٧) من ميثاق الحقوق الأساسية للاتحاد الأوروبي من استحقاق الأفراد لمحاكمة عادلة والتمثيل أمام القضاء[٢].

إلا أنه يجب الانتباه هنا إلى أن هذا المطلب وإن كان جوهريًّا من حيث المبدأ، والولايات المتحدة بإمكانها نظريًّا أن توفره بأن يتم إقرار تعديل قانوني يوفر الحماية القضائية لأصحاب البيانات أو ما شابه، إلا أنه من الناحية العملية قد يعتبر مطلبًا فارغًا من مضمونه. ذلك لأن فكرة لجوء أصحاب البيانات الأوروبيين للقضاء في قارة أخرى

(1) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), article 87.

(2) Recitals 141 and 143 of the GDPR.

(أمريكا الشمالية) هي مسألة مشوبة بمشقات ونفقات عالية قد تجعل منها سبيلاً غير عملي، يتعذر معه الحصول على حماية عملية، وهو ما يضعنا أما التساؤل حول ما إذا كان مطلب توفير سبل الإنصاف القضائي مطلبًا شكليًا، وبالتالي يكفي لتوافره تعديل تشريعي على نحو ما ذكرنا، أم أنه مطلب موضوعي لا يتحقق إلا إذا كانت آليات الإنصاف القضائي فعالة يمكن للمتضررين الوصول إليها والاستفادة منها بما يحقق عدالة فعلية.

بخلاف ذلك، الحكم لم يكن واضحًا بخصوص كيف يكون الامتثال ملائمًا أو كافيًا. انتهت المحكمة إلى بطلان درع الخصوصية لما لسلطات الاستخبارات من سلطات، ولعدم توفير حقوق قابلة للإنفاذ وسبل إنصاف قانوني ملائمة، وقررت كذلك صحة البنود القياسية في ذاتها، إلا أنها آثرت أن تكتفي بهذا الحد، دون أن تبين ما هي التدابير التي يمكن اتخاذها لتصحيح اتفاقية نقل البيانات، ودون أن تحدد معايير أكثر دقة يمكن للطرفين الأوروبي والأمريكي الامتثال لها بالنسبة لاتفاقية نقل البيانات أو للبنود القياسية. إلا أن هذا المنحى ليس غير ذي منطق. فالمحكمة إذا أوصت بتدابير معينة لتفادي أخطاء قرار الملاءمة أو لتدعيم البنود الاتفاقية، تكون قيد قيدت نفسها بهذه التدابير إذا ما أثبت الواقع العملي عيبًا فيها. ذلك بالإضافة إلى أنها ليست وظيفة المحكمة على أي حال أن تقيد صناع السياسة بتدابير سياسية أو إدارية ترتئيها، وإنما يقتصر دورها على أن تمارس رقابتها القضائية عليها في حدود ما يسمح به القانون، وبعد أن تعبر السلطة التنفيذية عن إرادتها بشكل كامل. ذلك التصور هو تطبيق مجرد لمبدأ الفصل بين السلطات.

السؤال الذي يطرح ذاته هنا هو ما إذا كان يمكن لقرارات الكفاية التي تصدر لصالح الولايات المتحدة أن تتغلب على العيوب التي تمت ملاحظتها في قرار شريمز ١، وتم التأكيد عليها في شريمز ٢، وذلك دون تغيير في قوانين الولايات المتحدة الطعينة. وهنا تكمن أهمية الحكم في أنه وضع المفوضية الأوروبية والحكومة الأمريكية في مأزق، إذ يفترض بالأخيرة إدخال تعديلات في نظامها القانوني مما يحد من سلطات نشطات الاستخبارات. كما يتوجب استبدال آلية محقق الشكاوى بأخرى ذات صبغة قضائية، بأن يتم إنشاء محكمة تختص بشأن بحث حماية البيانات على سبيل المثال.

وواقع الأمر أن المحكمة قد تجنبت الفصل في مدى صحة نقل البيانات من خلال

البنود القياسية للولايات الأمريكية، واكتفت بالبت في صحة البنود التعاقدية القياسية ذاتها، وانتهت إلى أنها ذاتها بشكل مجرد صحيحة على ما رأينا. ذلك المسلك قد يكون مقبولًا بالنسبة للبنود القياسية؛ نظرًا لأن البنود القياسية هي مجرد نموذج عقدي، لذا فمسألة صحتها هي مسألة موضوعية مجردة. ذلك يختلف عن صحة تطبيق البنود، فتلك مسألة فردية يتم بحثها في كل حالة على حدة. ولذلك فمن الوارد أن يمكن لناقلي البيانات اتخاذ تدابير إضافية لحماية البيانات فوق ما تنص عليه البنود القياسية لتلافي المخاطر التي تحدق بها. ذلك يمكن أن يكون في صورة تعتيم للبيانات (Anonymization) أو استخدام اسم مستعار (Pseudonymization) على سبيل المثال، مما يصعب مهمة وكالات الاستخبارات أو يجعلها مستحيلة على حسب الأحوال. إذا كانت البنود التعاقدية تسمح بهذه المرونة، لأن طبيعتها تعاقدية وتطبيقها يكون على مستوى فردي، إلا أن ذلك لا يتوافر بالنسبة لقرار الكفاية. ذلك أنه كما ذكرنا سلفًا قرار ينطبق بشكل مباشر، ويغني عن أي ضمانات فردية، وهكذا لا يتم الفصل بين مسألة صحة القرار وصحة تطبيقه، فهذا يجُبُّ ذاك.

إذا كان الأمر كذلك، فإنه لا يمكن القول بأن قرار الكفاية صحيح إلا إذا كانت قوانين الدولة وتنظيمها القانوني يوفر مستوى مساوٍ من الحماية، وهو ما لا يغني عنه ولا يمكن فيه اتخاذ تدابير لاحقة لتدارك عيوبه. مما يضحى معه السبيل المنطقي الوحيد أمام ناقلي البيانات هو إحداث إصلاحات قانونية في القوانين والقرارات المعنية في الولايات المتحدة.

كنتيجة لحكم شريمز ٢، مبدأ توطين البيانات أصبح محل اهتمام (Data localisation). توطين البيانات تفرض من خلاله الدول على المتعاملين في البيانات الشخصية عدم نقلها إلى خارج حدود الدولة، بأن يكون ذلك بنص صريح في القانون أو ضمنًا عن طريق قيود أخرى غير مباشرة تجعل عملية نقل البيانات إلى الخارج غير ممكنة عمليًّا. مثال ذلك أن يتم إلزام الشركات بعمل نسخة محلية، على أرض الدولة، من البيانات قبل نقلها، أو أن تحتفظ بنسخة من البيانات لمدة معينة في الدولة، أو أن يتم إلزامها بالقيام بالمعالجة على أرض الدولة كذلك، أو أن يشترط الحصول على موافقة الدولة والجهات التابعة لها.[1] وفي ذلك لا تلتزم الدول نهجًا واحدًا في حظر

(1) Cory N, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" <https://itif.org/pub-

نقـل البيانات، فمنهم مـن يضع حظرًا شاملًا لكل أنواع البيانـات والخدمات، والبعض يستهدف أنواعًا دون غيرها.

ذلك النوع من السياسة المناوئة لنقل البيانات للخارج قد يكون الهدف منه – بخلاف مـا ذكر سلفًا– هو الحد من ولوج الاستثمار الأجنبي إلى السوق الوطنية، بهدف حماية الصناعـات والاستثمارات الوطنية، ذلك أن البيانات الشخصية أمست بوابة الاستثمار للأسواق المحلية، كما أنها ركيزة له على المدى الطويل، ففهم احتياجات السوق وتوجهات المستهلكـين، وبالتـالي مـدى القابلية للاستثمار لا تقـوم كلها إلا ببحـث للسوق، والذي يعتمد بـدوره على دراسة البيانات الشخصية، وذلك بالطبع بخلاف الأنشطة التجارية التي يكون قوامها هو البيانات الشخصية ذاتها[١].

قـد يتبادر إلى الذهـن التساؤل حول مـا إذا كان توطين البيانات هـو الحل الأنسب فـي ظـل حكم شريمز٢، ومـا إذا كان هذا الحكـم يعد بمثابة قرار غـير مباشر بوقف نقـل البيانات لخارج الاتحاد الأوروبي. إلا أن هذا مـردود عليه بأن احتياجات التجارة العالمية تجعله شبـه مستحيل أن يقوم الاتحاد الأوروبي بتوطين بيانات مواطنيه، خاصةً مـع حليف بحجم الولايات المتحدة، فكثير من الخدمـات والنماذج التجارية تعتمد على شـراكات خارجيـة للوصول إلى منتجهـا النهائي. ذلك له صور عديـدة بينها التخزين السحابـي مثـلًا أو حتـى استخـدام موظفـين أو شـركات خدمة عملاء عـبر الحدود. بالإضافة إلى ذلك، فتوطين البيانات عملية مكلفة للغاية، واللجوء إليها قد يعطي مزية لبعض الأنشطة التجارية المحلية دون غيرها[٢].

lications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost/> accessed September 17, 2021.

(١) ذهـب أحـد التقديرات إلى أن البيانات العابرة للحدود أضافت للناتج المحلي الإجمـالي العالمي قرابة الـ ٢.٤ تريليونات دولار أمريكي في عام ٢٠١٤ وحده، Globalisation in transition: The future of trade and value chains.

(2) Chander A, "Is Data Localization a Solution for Schrems II?" (2020) 23 Journal of International Economic Law 771.

الخاتمة

هذا الحكم ينبغي النظر له باعتباره خطوة في سلم سبقه درجات أخرى وليس قفزة في ذاتها. فهو نتيجة لقضية شريمز ١، وبناء يجد أساسه فيه، إذ إن نشاط ماكس شريمز وتسريبات سنودن، وما تلاهما من نظر محكمة العدل الأوروبية في مدى صحة الملاذ الآمن، ومدى حق الأفراد في الشكوى من انتهاك نقل البيانات لحقوقهم، وكذلك التطور في تعاطي المفوضية الأوروبية للشكاوى المتعلقة بانتهاكات البيانات الشخصية قد مهد الطريق لهذا الحكم. وكذلك لا يمكن إنكار دور التطورات التي أتت بها اللائحة العامة لحماية البيانات الشخصية، إذ أضافت تحديدًا أكثر على عملية حماية بيانات مواطني الاتحاد الأوروبي؛ فجعلت هناك إطار من المبادئ لحكم كل عمليات معالجة البيانات، وأتاحت وجود آلية للتنفيذ والمراجعة. ذلك التطور مما يمكن تشبيهه بعدسة حسنت رؤية الفاعلين في مجال حماية البيانات – بما في ذلك محكمة العدل الأوروبية – للحدود المفترضة للتعامل في البيانات الشخصية.

لذلك فالمؤكد أن هذا الحكم هو لبنة في بناء لم يتم الانتهاء منه. فمجال حماية البيانات الشخصية مازال لم يكشف عن كل ما تحويه جعبته بعد. وهذا الحكم جاء ليصحح الاتجاه فيما يخص نقل البيانات للخارج، وهي مسألة شديدة الحيوية بالنسبة للمجال ككل؛ لأنه يصعب على دولة طبيعية في عصر المعلومات هذا أن تحبس كل بيانات مواطنيها بالرغم من كل الاعتبارات التجارية والاقتصادية.

أعطت محكمة العدل الأوروبية في هذه القضية القوانين الأمريكية نصيب الأسد من اهتمامها، وتحديدًا قوانين الاستخبارات[1]. كان على المحكمة الفصل فيما إذا معالجة البيانات عند نقلها لأغراض الأمن القومي سلطات الأمن القومي يمثل استثناءً من نطاق تطبيق اللائحة العامة لحماية البيانات. رأت المحكمة أن المعالجة على هذا النحو لا تقيم أي من الاستثناءات التي نصت عليها المادة (٢) من اللائحة. النقل من فيس بوك أيرلندا إلى فيس بوك الأم في الولايات المتحدة هو عملية نقل بيانات بين كيانين اقتصاديين لأغراض تجارية، وبالتالي يتقيد بأحكام اللائحة.

تناولت المحكمة كذلك نقل البيانات بواسطة البنود التعاقدية القياسية، وتحديدًا

(1) Julia Hamilton, ‹Data Prot. Comm›r v. Facebook Ireland Ltd. and Maximillian Schrems: Shattering the International Privacy Framework› (2021) 29 Tul J Int›l & Comp L 351

ماهية المعايير التي تحقق بها البنود مستوى حماية ملائم. وقررت في ذلك أنه لا بد من توفير ضمانات كافية، وحقوق قابلة للإنفاذ لصاحب البيانات، وسبل إنصاف قانوني. وإذ أكدت المحكمة على فكرة المستوى الحماية المساوي باعتباره ركيزة نقل البيانات، فقد بينت أن ذلك المفهوم لا يعني التطابق بين النظامين القانونيين، وإنما التساوي في جوهر الحماية القانونية.

حدد الحكم كذلك حدود اختصاص السلطات الإشرافية إذا ما تراءى لها وجود مخالفة ما. الحد الأدنى للاختصاص هو أنها تستطيع أن تتلقى الشكاوى سواءً كان النقل بواسطة قرار ملاءمة أم البنود القياسية. وفي حالة البنود القياسية يتوجب عليها أن تقرر وقف نقل البيانات أو إنهاءه في حالة تعذر الامتثال لضوابط النقل. لكنه بالنسبة لقرارات الملاءمة فإنه ليس لها الأمر بذلك، إلا أنها تستطيع رفع الأمر للمحكمة التي تستطيع إحالة المسألة المتنازعة لمحكمة العدل الأوروبية.

فيما يتعلق بصحة قرار اعتماد البنود القياسية، فقد كان قرار المحكمة أن البنود ذات طبيعة تعاقدية خالصة، لذلك من غير المتوقع فيها إلزام السلطات العامة في دولة أجنبية، ولا يعد ذلك معيارًا لصحتها. لكن مسئولية التأكد من تطبيق البنود تطبيقًا صحيحًا والتأكد من ملاءمة مستوى الحماية في الدولة مستقبلة البيانات، وكذلك مدى قدرة مستقبل البيانات على الإذعان للبنود تقع على المتحكم أو المعالج مصدر البيانات. وبالتالي فالأخير يتوجب عليه اتخاذ تدابير إضافية للتحوط ضد أخطار البيانات في الدولة مستقبلة البيانات.

أكبر نتائج الحكم هو القضاء بإبطال قرار درع الخصوصية للمثالب التي يعاني منها النظام القانوني الأمريكي، خاصةً قوانين الاستخبارات الخاصة بها. إذ رأت المحكمة أن هذه القوانين لا تكفل مستوى حماية كاف، حيث تستطيع أجهزة الاستخبارات جمع بيانات الأوروبيين بكميات كبيرة، كما تستطيع أن تجمع البيانات التي تمر عبر الولايات المتحدة دون أن تكون خاضعة لرقابة القضاء في ذلك. وفوق ذلك قررت المحكمة أن آلية متلقي الشكاوى لا تستوفي متطلبات سبل الإنصاف القانوني والقضائي، نظرًا لعدم استقلاله وعدم إلزامية قراراته في مواجهة السلطات العامة الأمريكية.

في ضوء هذا أصبحت كافة الشركات والمؤسسات التي تنقل البيانات أن توقف النقل

الـذي يتم وفق قـرار الملاءمـة درع الخصوصية. وبالتالي مع عدم وجـود قرار ملاءمة تغـدو الوسيلة الأنسب من بين وسائل المادة (٤٦) مـن اللائحة العامة لحماية البيانات الشخصيـة لنقل البيانات هي البنـود التعاقدية القياسية. وهو الحـال منذ تاريخ ذلك الحكم وحتى وقت كتابة هذه السطور. والمحاولات جارية أيضًا منذ ذلك الوقت للوصول إلى اتفاقيـة نقـل بيانات جديدة، كما أن مجلس حمايـة البيانات الأوروبي (European Data Protection Board (EDPB) قـد بادر بإصدار توصية بالتدابير التي ينبغي على مصدري البيانات اتباعها في ظل حكم شريمز ٢ لتحقيق عملية نقل سليمة.

لكنـه عمومًا إذا كانت البنود التعاقدية حلاً للوضع الحالي، فإنها حل مرهق ومؤقت وذلك لأنها – وكما أوضحت المحكمة – تترك كلًا من المتحكم والمعالج تحت عبء التحقق مـن شرعية عمليـات النقل كلٍ على حـدة، أي أنه يتوجب على مرسـل البيانات وكذلك مستقبلهـا أن يفحـص كل عملية نقل بشكل مستقل، وهو ما يترتـب عليه ضغط قانوني مستمر للتحقق من صحة عمليات النقل، وتهديد أكبر لها بالإبطال حال تمامها[1].

(1) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, adopted on 18 June 2021.