توطين البيانات(دراسة قانونية مقارنة)

د. عبد العزيز بن أحمد المزيني

أستاذ مساعد بقسم السياسة الشرعية

المعهد العالي للقضاء - جامعة الإمام محمد بن سعود الإسلامية

مقدمة

يعيش العالم اليوم تطورا تقنيا مذهلا ومتسارعا، فلا يكاد الإنسان يدرك شيئا من هذا التطور إلا ويكتشف أن ثمة مجالات أخرى سبقته. وهذا التطور التقني في مجالات متعددة: مدنية، وعسكرية، وأمنية، وتعليمية، وجوانب أخرى لا يمكن حصرها. ومن أهم الجوانب التي واكبت هذا التطور التقني: وفرة البيانات وغزارتها وسهولة الحصول عليها ومعالجتها وتحليلها.إن الوفرة الحالية في البيانات وغزارتها لم تكن بهذه السهولة من قبل، وإنما مرت بمراحل عديدة حتى وصلت إلى ما وصلنا إليه الآن، فرغم وجود الإنترنت من التسعينات الميلادية إلا أن الأفراد كانوا يستخدمون حواسيبهم الشخصية لتخزين البيانات التي يحصلون عليها – أو التي ينشئونها – أو يخزنونها في أجهزة إضافية ملحقة بهذه الحواسيب. أما الشركات والمؤسسات فكانت تستخدم خوادم خاصة موجودة في مقر كل شركة لتخزين بيانات الشركة وبيانات العملاء، ومن ثم معالجتها والعودة إليها متى لزم الأمر. وعند تراكم البيانات تصبح هذه الأجهزة أو الخوادم الخاصة غير كافية لتخزين البيانات الموجودة، ما يستدعي حذف الزائد أو توسيع المكان للتخزين، وقد لا يستوعب تخزين البيانات الزائدة مقر الشركة أو بيت الفرد.ولذلك فإن أمكِنة تخزين البيانات في السابق كانت محدودة، وبالتالي فصناعة البيانات كانت محدودة كذلك، إلى أن أطلقت شركات التقنية الكبرى تقنية جديدة، تسمى التقنية السحابية (cloud)، والمقصود بها: تخزين البيانات والمعلومات عند شركة التقنية بدلا من تخزينها في الحواسيب الشخصية أو الخوادم الخاصة، ومن الشركات التي تقدم هذه التقنية السحابية آبل Apple و جوجل Google و مايكروسوفت Microsoft، وباستخدام هذه التقنية السحابية لا يضطر الفرد أو الشركة الخاصة أو المؤسسة لتجهيز مكان أو توفير أجهزة لتخزين البيانات؛ بل ستقوم شركة التقنية بتخزين البيانات كاملة عندها بالنيابة عنه. ولتخزين البيانات لدى شركات التقنية فوائد عديدة؛ أولا: أنها أوفر من الناحية المادية، حيث يدفع المشترك رسوما شهرية محددة مقابل تخزين البيانات بدلا من تحمّله قيمة شراء الخوادم التي تبينها الشركات في مقارها أو الاضطرار لشراء حواسيب جديدة للأفراد. ثانيا: لن يحتاج الفرد أو الشركة إلى مساحة أو حيّز يستقطعه لتوفير مكان للتخزين، حيث يعد هذا عبئا كبيرا خاصة للشركات الكبيرة، ويتخلص المشترك كذلك من عبء الصيانة والمتابعة لهذه الأجهزة الحساسة. وأهم فائدة مرجوة من التخزين السحابي تتمثل في أنه لم يعد هناك حدّ لتخزين البيانات، فكلما زاد الاحتياج كان المطلوب فقط هو دفع رسوم إضافية لمقدم الخدمة السحابية ليرفع سعة التخزين. وبسبب ذلك حدثت ثورة في صناعة البيانات؛ إذ لم يعد لتخزين البيانات وحفظها ومعالجتها حدّ، وتضاعَف حجم البيانات في السنوات الأخيرة بشكل مهول بسبب هذه التقنية السحابية.[1]ولكن هذه البيانات وإن كانت سحابية بالنسبة للفرد أو الشركة إلا أن شركات التقنية التي تقدم هذه التقنية السحابية لا بد أن توفر مراكز لتخزين البيانات التي حصلت عليها من مختلف المستخدمين، وبالطبع، ستكون هذه المراكز كبيرة الحجم وتحتوي على كميات ضخمة جدا من البيانات بمختلف أنواعها ومن مختلف دول العالم. ولهذا شرعت شركات التقنية في بناء تلك المراكز في بقاعٍ شتى من الأرض. ومعنى ذلك، أنه صار هناك طرف ثالث في عملية الوصول للمعلومة، أي أن "هناك وسيط هو مزود الخدمة السحابية يعمل في المنتصف بين مالك البيانات والبيانات. فإذا رغب مالك البيانات في التحكم بالبيانات، فإن ذلك يعتمد على ما إذا كان هذا "الوسيط" يفي بأمانة بالتزاماته كوكيل".[2]ومن هنا ظهر النقاش حول مكان تخزين هذه البيانات وحفظها؟، ولأيّ اختصاص قانوني تخضع تلك البيانات المحفوظة لدى مزود الخدمة السحابية إذا كانت مراكز التخزين في بقاعٍ شتى من الأرض؟ كما ظهرت أسئلة أخرى حول المستفيد ماليا واقتصاديا من تخزين البيانات؟، ولماذا نجد أن شركات التقنية الكبرى هي المستفيدة من هذه البيانات وحدها؟، وما الذي يضمن أن هذه البيانات محمية من أي اختراقات أو أنها لا تُستغلّ من دول أخرى قد تكون عدوة أو على الأقل غير صديقة؟ وتصاعدت إثر هذه الأسئلة الدعوات إلى توطين البيانات من قبل بعض الدول، وصدرت بالفعل قوانين عديدة من بعض الدول تشترط توطين البيانات التي علاقة بأفراد ومواطني هذه الدول، والذي هو مناط هذا البحث.

أهمية البحث

تكمن أهمية البحث في أهمية ما يتناوله، وهو البيانات نفسها، وخطورتها السياسية والاقتصادية والاجتماعية في الزمن المعاصر، فهي نفط العصر الجديد، وتشكل موردا اقتصاديا وماليا ضخما للشركات والدول. وما تضخمت القيم المالية للشركات التقنيّة الكبرى،مثل:فيسبوك،وتويتروغيرها، إلا بسبب حيازتها لكميةِ بياناتٍ هائلة. بالإضافة إلى أن البيانات تشكل أمنا وطنيا للدول، فالمستحوذ على البيانات لديه معلومات كثيرة عن أفراد أي دولة، وبالتالي يمكنه تحليل هذه البيانات والاستفادة منها في أي خطط عدائية تهدد الأمن الوطني. كما أن البيانات تحتوي على معلومات الأفراد الخاصة والشخصية، سواء البنكية منها أو الصحية أو الاجتماعية، وفي تسريبها أو استغلالها

ضرر على الأفراد، ومن ثمّ على المجتمع كله. ولهذا تشترط بعض الدول توطين البيانات للتأكد من ضمان سلامة البيانات من هذه المخاطر، ومن هنا تنبع أهمية البحث.

مشكلة البحث

تختلف التوجهات الدولية في توطين البيانات، فبعض الدول ألزمت الشركات بالتوطين بشكل إجباري،وبعضها في الطرف الآخرلم تجبر الشركات على توطين البيانات بل منعته.ومن هناتأتي المشكلة التي يريدأن يعالجها البحث:هل الأفضل للدول توطين البيانات أو الأفضل عدم ذلك؟ وذلك من خلال مقارنة هذه التوجهات من الناحية التشريعية وتحليل الإيجابيات والسلبيات في كل توجه، ومحاولة فهم أسباب تبني الدول لهذه التوجهات وسبب اختلافها فيه، ومن ثمّ الوصول إلى نتيجة حول أفضل التوجهات،من خلال تفاصيل عدة تتبين في ثنايا البحث بإذن الله

نطاق البحث ومنهجيته

يقتصر نطاق البحث على دراسة التوجهات التشريعية العامة في توطين البيانات، وذكر أهم الدول التي تتبنى كلّ توجه، ولذلك فالبحث لا يدخل في التفاصيل الدقيقة والشروط الخاصة التي تنصّ عليها القوانين فيما يتعلق بتوطين البيانات، وإنما ينحصر في دراسة التوجهات التشريعية العامة، إضافة إلى تحليل هذه التوجهات ومعرفة الأسباب التي دعت الدول لتبنيها والآثار الإيجابية والسلبية والمقارنة بينهاوعليه، فالبحث يتبنى المنهج المقارن والمنهج التحليلي، وذلك بالمقارنة بين التوجهات التشريعية العامة، وتحليل هذه التوجهات من ناحية آثارها والأسباب الداعية لها: الاقتصادية والسياسية، والمقارنة بينها وترجيح الأنسب منها من وجهة نظر الباحث.

خطة البحث

يشتمل البحث على هذه المقدمة، وثلاثة مباحث، وخاتمة. يتناول المبحث الأول تعريف توطين البيانات لغويا واصطلاحيا، وتحديد معنى البيانات المقصود عند ذكر مصطلح توطين البيانات، وعلاقة توطين البيانات بمبدأ سيادة الدولة. في حين يتناول المبحث الثاني الإيجابيات والسلبيات المترتبة على توطين البيانات والمقارنة بينها. أما المبحث الثالث فيتناول التوجهات الدولية التشريعية في توطين البيانات من حيث الإلزام من عدمه، وموقف بعض الدول العربية من ذلك. وانتهى البحث بخاتمة تشتمل على أهم النتائج والتوصيات.

المبحث الأول: التعريف بتوطين البيانات وعلاقته بمفهوم السيادة

المطلب الأول: تعريف توطين البيانات لغة واصطلاحا:

- تعريف التوطين لغة: مأخوذ من الفعل (وَطَّنَ، يوطِّن، تَوطينا)، يقال: وَطّن فلانا، أي: أنزله سكنا يقيم فيه[٣]، ويستخدم لفظ التوطين كترجمة لكلمة Localization، أما Localizationباللغة الإنجليزية فهي مأخوذة من كلمة Local، وهي صفة تحمل معنى نسبة الشيء أو الشخص إلى مكان، أي أن له صفة مميزة لها علاقة بالمكان أو بالموقع، وقد رأينا أن أنسب ترجمة لها في سياق موضوع البحث هي كلمة "توطين"؛ لعلاقتها الوثيقة بالمكان المحدد، والذي هو في سياق البحث: الدولة ذات السيادة، المحدد مكانها في بقعة جغرافية معلومة.
- تعريف البيانات لغة: كلمة البيانات هي ترجمة لكلمة Data، والبيانات في اللغة العربية المعاصرة تعني "معلومات تفصيليّة حول شخص أو شيءٍ ما يمكن من خلالها الاستدلال عليه"، وفي السياق الحاسوبي تدل على "رموز عدديّة وغيرها من المعلومات الممثَّلة بشكل ملائم لمعالجتها بالحاسوب"[٤]. وكلمة Dataفي اللغة الإنجليزية تحمل المعنى نفسه.
- تعريف توطين البيانات اصطلاحا:كما بينا في المقدمة، فإن مصطلح توطين البيانات مصطلح حديث، ولهذا تجد العديد من التعريفات التي تناولت هذا المصطلح، وقد تختلف هذه التعريفات فيما بينها، ما يصعّب الوصول إلى تعريف محدد ودقيق، بالإضافة إلى أن مصطلح توطين البيانات قد يكون له أكثر من مفهوم باختلاف قوانين الدول التي تتعامل معه، ولتحقيق أهداف هذ البحث، فإن التعريف الذي نراه مناسبا هو: "المتطلَّب القانوني أو الإداري المُلزم الذي ينصّ بصورة مباشرة أو غير مباشرة على تخزين البيانات أو حتى معالجتها ضمن حدود الدولة، سواء أكان ذلك بصورة حصرية أم بصورة غير حصرية".[٥]يُلحظ في التعريف أنه فرّق بين المتطلبين القانوني والإداري، وهذا تفريق دقيق ومقصود، وذلك ليشمل ما فُرض بنصّ قانوني أو لائحي صادر من السلطة التشريعية في كل دولة بحسبها، أو ما فرض بقرار إداري صادر من السلطة التنفيذية بهدف تنظيم عمل الجهات التابعة لها، وذلك مثل ما تفرضه مثلا بعض وزارات الصحة على المستشفيات من تخزين معلومات المرضى في الدول نفسها، ولا تسمح بنقلها خارج الدولة، أو ما تفرضه بعض الجهات الحكومية على منسوبيها من تخزين المعلومات الخاصة بها داخل الدولة ولا يسمح بنقلها خارجها، وغير ذلك من الأمثلة التي ستتضح في ثنايا البحث بإذن الله.

كما فرّق التعريف بين الأمر المباشر وغير المباشر، والمقصود بالمباشر هو النص الصريح على تخزين البيانات داخل الدولة، أما غير المباشر فمثل الأمر بعدم نقل البيانات خارج الدولة إلا بإذن رسمي، فهذا أمر ضمني بتخزين البيانات داخل الدولة نفسهاوأوضح التعريف أيضا أن مصطلح توطين البيانات لا يقتصر على حفظ البيانات فقط داخل الدولة، بل حتى على معالجة البيانات، مثل تحليلها وربطها، يدخل ضمن مصطلح التوطين، إذ إن عددا من الدول تشترط أن معالجة البيانات يجب أن يتم داخل الدولة، ولا تجوز معالجة البيانات خارج الدولة إلا بإذن رسمي، كما سيتضح ذلك لاحقا بإذن الله.وأخيرا، بيّن التعريف أن توطين البيانات قد يكون بصورة حصرية أو بصورة غير حصرية، حيث إن بعض الدول تشترط تخزين البيانات داخلها وتمنع تخزينها خارجها، وبعض الدول تسمح بتخزين البيانات خارج الدولة، ولكن لا بد من وجود نسخة من هذه البيانات داخل الدولة.

المطلب الثاني: نطاق البيانات المقصود بالتوطين

من المهم جدا قبل الولوج في ثنايا البحث معرفة المقصود بالبيانات، والنطاق الذي تشمله البيانات عند ذكر مصطلح توطين البيانات، هل يشمل جميع البيانات الموجودة في الأجهزة الإلكترونية وشبكة الإنترنت المستهدفة بالتوطين؟ أم أن هناك بعض الأنواع التي يشملها التوطين دون غيرها؟ولتوضيح المقصود بالبيانات عند ذكر مصطلح توطين البيانات، يمكن تقسيم البيانات إلى ثلاثة أقسام:

القسم الأول يشمل "بيانات الدولة التي تندرج تحت فئة الأمن الوطني محليا؛ إذ تحتاج المستندات الحكومية السرية والبيانات العسكرية وغيرها من المستندات السرية للدولة عادةً إلى تطبيق سياسات صارمة لتوطين البيانات".[٦] ولهذا تكاد تتفق الدول –حتى الدول التي تعارض توطين البيانات بشدة– على أن هذا النوع من البيانات يجب أن يتم تخزينه وتوطينه في البلد نفسه وذلك لعلاقته الشديدة بالأمن الوطني. وذلك مثل الولايات المتحدة الأمريكية –وهي من الدول التي تعارض توطين البيانات– فإن وزارة الدفاع الأمريكية تشترط على مزودي الخدمة تخزين جميع البيانات المتعلقة بها داخل الولايات المتحدة.[٧]

أما القسم الثاني، فهي بيانات متعلقة بالقطاع الخاص؛ لكنها "بيانات حساسة"، وبتعبير آخر تسمى بيانات ذات علاقة بـ"بنى تحية حيوية: ولذلك فإن لها تأثيرا مباشرا على الأمن والاقتصاد الوطني"، ولذلك فإن غالب تشريعات الأمن السيبراني في دول العالم تشترط تخزين هذه البيانات الحساسة في الدولة نفسها.[٨] ولتوضيح المقصود بالبيانات الحساسة، نذكر نموذجا وهو هيئة الأمن الوطني السيبراني السعودي، حيث أصدرت ضوابط خاصة بهذا النوع من البيانات وهي "ضوابط الأمن السيبراني للأنظمة الحساسة"[٩]، وعرّفت هذه الضوابط الأنظمة الحساسة بأنها "أي أنظمة أو شبكات، يؤدي تعطلها، أو التغيير غير المشروع لطريقة عملها، أو الدخول غير المصرح به لها، أو للبيانات والمعلومات التي تحفظها أو تعالجها؛ إلى التأثير السلبي على توافر الخدمات، أو أعمال الجهة العامة، أو إحداث آثار اقتصادية أو مالية أو أمنية، أو اجتماعية سلبية كبرى، على المستوى الوطني"[١٠]، ثم ذكرت الضوابط المعايير التي من خلالها تقيم هذه الآثار السلبية، وهي: "١) التأثير السلبي على الأمن الوطني، ٢) التأثير السلبي على سمعة المملكة وصورتها العامة، ٣) خسائر مالية كبرى (مثال: أكثر من ٠.٠١٪ من إجمالي الناتج المحلي الوطني)، ٤) التأثير السلبي على خدمات مقدمة لعدد كبير من المستخدمين (مثال: أكثر من ٥٪من التعداد السكاني)، ٥) خسائر في الأرواح، ٦) الإفشاء غير المصرح به لبيانات يكون تصنيفها سريا أو سريا للغاية، ٧)التأثير السلبي على أعمال قطاع حيوي أو أكثر"[١١].وفقا لهذه الضوابط، فإن تحقق أي من هذه المعايير يجعل البيانات ذات علاقة بالأنظمة الحساسة، وبالتالي يجب تطبيق أحكام وضوابط خاصة –من ضمنها تخزينها في البلد نفسه– حتى لو كانت هذه البيانات ذات علاقة بالقطاع الخاص، مثل بيانات شركة الكهرباء، وشركات الاتصالات، وتوزيع الوقود بين المحطات، وغيرها. هذه كلها يجب تخزينها في البلد نفسه لأن أي ضرر بها سينتج عنه آثار وخيمة على اقتصاد البلد وأمنه الوطني.

أما القسم الثالث، فهي البيانات التي تتعلق بالقطاع الخاص والأفراد، وليس لها علاقة بالأنظمة الحساسة والبنية التحتية الحيوية، وذلك مثل "رسائل البريد الإلكتروني، وملفات التعريف في وسائل التواصل، وأنماط استخدام التطبيقات عبر الإنترنت، وجميع البيانات الناشئة عن استخدام الأفراد للإنترنت".[١٢] وغالبا ما يقصد بالبيانات عند إطلاق مصطلح توطين البيانات، البيانات الشخصية المتعلقة بالأفراد، نظرا لتعلقها بخصوصية الأفراد، ولذلك صدرت العديد من القوانين الدولية التي تنظم وتحمي بيانات الأفراد وعلى رأس هذه القوانين: القانون العام لحماية البيانات الصادر عن الاتحاد الأوروبي (General Data Protection Regulations "GDPR")، حيث إن الهدف من هذا القانون – حسب ما نصت المادة الأولى منه– أنه "يضع القواعد المتعلقة بحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية والقواعد المتعلقة بحرية حركة البيانات الشخصية."[١٣] فالقانون إنما هو لحماية البيانات الشخصية المتعلقة بالأفراد لحماية خصوصياتهم، وهو صادر

عن الاتحاد الأوروبي وملزم لكل الدول التابعة للاتحاد وللشركات التي تخدم مواطني ومقيمي هذه البلاد، كما سيأتي تفصيل ذلك لاحقا. ونحا منحى الاتحاد الأوروبي في وضع نظام أو قانون يحمي البيانات الشخصية العديد من الدول، ومثال ذلك المملكة العربية السعودية في إصدارها لنظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم م/١٩ وتاريخ ١٤٤٣/٢/٩هـ، والذي نص في مادته الثانية على أنه "يُطبق النظام على أي عملية مُعالجة لبيانات شخصية تتعلق بالأفراد تتم في المملكة بأي وسيلة كانت، بما في ذلك معالجة البيانات الشخصية المتعلقة بالأفراد المقيمين في المملكة بأي وسيلة كانت من أي جهة خارج المملكة."[١٤] ومثله قانون حماية البيانات الشخصية الصيني (Personal Information Protection Law) الصادر في عام ٢٠٢١م، والذي ينص في مادته الأولى على أنه قد "تم سن هذا القانون وفقا للدستور لحماية حقوق ومصالح البيانات الشخصية، وتنظيم معالجة البيانات الشخصية، وتعزيز الاستخدام المعقول للبيانات الشخصية."[١٥]والسبب في تركيز الحكومات على البيانات الشخصية بالذات هو حماية خصوصية الأفراد من استغلال الشركات، إذ إن الشركات التي لديها هذه البيانات أصبحت لديها قدرة وقوة لا تملكها الحكومات نفسها، بسبب تراكم هذه البيانات عندها، فمثلا "وفقًا لنتائج شركة "علي بابا" Alibaba ربع السنوية في نهاية سبتمبر ٢٠١٦م الصادرة في ٢ نوفمبر ٢٠١٦م، بلغ عدد المشتركين النشطين على منصة "تاوباو" Taobao الصينية ٤٣٩ مليونًا. ووفقًا لسياسة الخصوصية في "تاوباو"، يُطلب من المشترين من "تاوباو" تقديم المعلومات التالية على الأقل: الاسم، والجنس، وتاريخ الميلاد، ورقم الهوية، واسم العائلة وفقا لجواز السفر، والاسم الأول وفقا لجواز السفر، ورقم جواز السفر، ورقم الهاتف، وعنوان البريد الإلكتروني...إلخ. وبالاستعانة بالمعلومات أعلاه، يمكن أن نقول إن شركة "علي بابا" تتحكم في المعلومات الشخصية الأساسية لـ ٤٠٠ مليون مواطن صيني على الأقل. وبمساعدة المشترين أثناء عمليات الدفع واستلام البضائع وغيرها من الحالات التي تربطها بالمشتري، يمكن أن نستنتج أن قدرة الشركة على التأكد من صحة البيانات وإدراكها لها يتجاوز إمكانات الحكومة."[١٦] وهذا مثال واحد فقط يبين القدرة الهائلة التي تملكها شركات التقنية الكبرى باستحواذها على هذا الكم الهائل من البيانات الشخصية، فكيف لو أضفنا لذلك فيسبوك وتويتر وسناب شات وغيرها.خلاصة القول، إن المقصود بالبيانات عند ذكر مصطلح توطين البيانات والاتجاهات القانونية المختلفة في توطين البيانات، هي البيانات الشخصية المتعلقة بالأفراد، كما نصت عليه القوانين المقارنة، وسيتضح ذلك أكثر في المباحث القادمة عند ذكر هذه الاختلافات.

المطلب الثالث: علاقة توطين البيانات بمفهوم السيادة

إن توطين البيانات والاتجاهات القانونية المتعلقة بها له علاقة وطيدة بمفهوم السيادة الوطنية، ولهذا لا بد من الإشارة إليه وإيضاح مدى التعارض أو التوافق بينهما، فالسيادة "مفهوم قانوني وسياسي، قديم قدم الدولة ذاتها"[١٧]، وأول من كتب عنها بالمعنى الحديث وجعل لها المعنى المعتمد حاليا في الدساتير والاتفاقيات الدولية "المفكر الفرنسي جان بودان في كتابه "ستة كتب عن الجمهورية" عام ١٥٧٦م، وترجع أهمية بودان إلى أنه أخرج فكرة السيادة نهائيا من سجن اللاهوت الأمر الذي أدى إلى إمكانية تناولها بالتحليل والدراسة، ومن ثم إدراجها في النظريات الدستورية، وأنه فصل بين الملك والسيادة، وجعلها عنصراً من عناصر تكوين الدولة."[١٨]ثم بعد ذلك "ارتبط نشوء الدولة ذات السيادة بنشوء الدولة القومية بعد معاهدة ويستفاليا سنة ١٦٤٨م، وقد أصبح هذا المفهوم أحد أهم أركان الدولة الحديثة، إذ يخولها احتكار أدوات القوة –بما فيها القمع والإكراه– لفرض سلطتها على كامل الإقليم الذي يشكل حدودها وعلى جميع الأفراد الذين يقطنون هذا الإقليم ."[١٩] فالسيادة إذن "صفة للسلطة، والسلطة ذات السيادة تشكل إلى جانب الإقليم والسكان أركان الدولة، ولا يمكن أن تكتمل الشخصية القانونية للدولة إلا بتوافر هذه الأركان الثلاثة".[٢٠]والسيادة لها مظهران: داخلي، وخارجي. أما المظهر الداخلي فيتمثل "بأن سلطة الدولة على إقليمها شاملة وسامية، لا تستطيع أي سلطة أخرى أن تعلو عليها في فرض إرادتها على الأفراد والهيئات داخل حدودها، أو في تنظيم شؤون إقليمها. فللدولة وحدها الحق الحصري في مباشرة كل الاختصاصات المتصلة بوجودها كدولة، وتمتع الدولة بالسيادة الداخلية يبرر احتكارها لأدوات القوة اللازمة لتمكينها من القيام بوظائفها في إدارة الشأن العام وفي التشريع والقضاء". أما المظهر الخارجي "فيتمثل في عدم خضوع الدولة لأية دولة أو سلطة أجنبية أخرى، بحيث تتمتع الدولة بالسلطة العليا عبر حدودها بما يؤمن استقلالها الكامل في مواجهة الدول الأخرى ويجعلها على قدم المساواة معها ".[٢١]هذا هو مفهوم السيادة المستقر لعشرات السنين، ولكن مع نهاية السبعينيات وبداية الثمانينيات، ونتيجة لتسارع عمليات العولمة، بدأ بعض علماء العلاقات الدولية الاعتقاد بأن الدول السيادية أخذت تفقد السيطرة على تحركات رؤوس الأموال والبضائع والبشر والشركات والمعلومات، ومن ثم بدأوا الحديث عن "أزمة السيادة" و"السيادة في خطر" و "السيادة في نهايتها". ومع تزايد قوة هذا الاتجاه ظهرت مقولات ترى أن مسلّمة "الدول بوصفها وحدات سياسية مستقلة آخذة في الانحسار في مواجهة الهجوم المتسارع لقوى العولمة مثل الاتحادات والإنترنت والشركات المتعددة الجنسيات والمنظمات غير الحكومية. وبدأ العديد من التحليلات الحديثة للاقتصاد السياسي العالمي طرح فكرة

أننا نعيش في مرحلة تحول ينفصل فيها الماضي عن المستقبل. فالعولمة الاقتصادية خلال ربع القرن الماضي كانت بداية لإعادة ترتيب حتمية ولا رجعة عنها لأدوار السياسة والاقتصاد، مع ازدياد خضوع الدول القومية لقوى السوق والاقتصاد العالميين والتقنية العالمية".[٢٢]ويظهر هذا جليا في موضوع البيانات بالذات، فالشركات العالمية، مثل تويتر وفيسبوك وسناب شات وغيرها، تستفيد من بيانات مواطني الدول، في تضخيم قيمها السوقية وتحقيق أرباح مليارية، من خلال تحليل تلك البيانات التي في حوزتها وبيع نتائجها للشركات الأخرى، والدول التي ينتمي لها أولئك المواطنون والمقيمون، لا تستفيد من تلك البيانات، بل وفي بعض الأحيان ليس لهم أي سيطرة عليها، بينما جميع المواد والسلع الأخرى التي لها وجود في أراضي الدول، يكون عليها على الأقل ضرائب ورسوم وقوانين تحمي تلك الموارد، ولهذا تولد الصراع بين سيادة الدولة على هذه المعلومات والبيانات الموجودة في أراضيها وتتعلق بمواطنيها، وبين حرية البيانات وتنقلها دون تدخل الدول فيها.وفي هذا الباب "نقاش طويل حول كيفية تأثير الإنترنت على السيادة وتأثره بها. ويبدو أن الاهتمام بهذا الموضوع قد ازداد خلال العامين الماضيين، وقد أثار هذا الموضوع مناقشات حول المعنى الجوهري للسيادة وكثيرا ما تتصاعد الدعوات إلى "سيادة البيانات"، و"سيادة المعلومات"، و "السيادة الرقمية"، و"السيادة التكنولوجية".[٢٣]فالدول بالطبع تدعو إلى سيادتها على هذه البيانات، بصفتها الحائزة أصالة لهذه البيانات، والشركات العالمية الرقمية تدعو إلى سيادة البيانات وعدم تدخل الدول فيها من باب حرية البيانات وحرية تدفقها. هذا الصراع أنتج اتجاهات قانونية مختلفة في توطين البيانات من عدمها، كما سنبين ذلك في المباحث القادمة بإذن الله.

المبحث الثاني: الآثار الإيجابية والسلبية المترتبة على توطين البيانات

مع التطور الاقتصادي والتقني الهائل الذي يعيشه العالم في هذا الزمن، من الصعب الحكم على توطين البيانات بشكل عام بأنه الأفضل للدول والمجتمعات أو أنه ليس كذلك؛ إذ يحفّ توطين البيانات العديد من الآثار والمبررات التي قد تختلف وجهات النظر حولها، وهل هي فعلا إيجابية أم سلبية، بل قد يكون ما هو إيجابي لدولة ما، سلبيا في الوقت نفسه لدولة أخرى (كما سيتضح ذلك لا حقا)، ومن الصعب أيضا سرد جميع هذه الآثار المتوقعة في هذا البحث، لذلك سنذكر أهم هذه الإيجابيات والسلبيات الجوهرية ثم نوازن بينها.

المطلب الأول: الإيجابيات المترتبة على توطين البيانات

يذكر المتخصصون في البيانات عددا من الإيجابيات لتوطين البيانات، وهي تنقسم إلى قسمين غالبا: أمني، واقتصادي، وإن كان الجانبان لا ينفكان عن بعضهما، إلا أن التقسيم من باب التقريب والتسهيل.أما الجانب الأمني، فمن أهم هذه الإيجابيات،

١. **حماية معلومات المواطنين الخاصة:**وهذا الجانب يعد من أهم الإيجابيات التي من أجلها حرصت الدول على اشتراط توطين البيانات في خضم إصدار الأنظمة والقوانين التي تحمي البيانات الشخصية للأفراد، ومن تلك القوانين الـ GDPR في الاتحاد الأوروبي، ونظام حماية البيانات الشخصية في المملكة العربية السعودية، وغير ذلك من الأنظمة والقوانين التي سيأتي ذكرها في المبحث القادم بإذن الله.والسبب في ذلك أنه في الواقع الحالي نجد أن معلومات الأفراد مخزنة في أنظمة سحابية تملكها الشركات الخاصة ومنتشرة في أنحاء العالم، وهذه البيانات تشتمل على العديد من البيانات الحساسة التي قد يكون في تسريبها ضرر كبير على الأفراد والمجتمعات[٢٤]، كما حصل ذلك لعدد من الشركات الكبرى والتي تسرب منها بلايين (ليس ملايين) المعلومات الشخصية. مثال ذلك ما حدث لشركة ياهو Yahoo الأمريكية عام 2013م، والتي كانت تعد ذلك الوقت من أكبر الشركات الأمريكية التقنية، حيث تسربت معلومات ثلاثة مليارات حساب تحتوي على معلومات حساسة مثل الاسم بالكامل والعنوان والبطاقة البنكية وغيرها،[٢٥] وأيضا كما حدث لشركة لينكد إن LinkedIn الأمريكية، وهي شركة تواصل مختصة بالمهنيين والمحترفين والتي تعد البوابة الأولى عالميا للبحث عن الوظائف، حيث تسربت معلومات ٧٠٠ مليون حساب في عام ٢٠٢١م، وتشتمل هذه المعلومات على معلومات حساسة[٢٦]، والأمثلة في ذلك كثيرة. لذلك تشرّع بعض الدول إلزامية توطين البيانات؛ للتأكد من أن معلومات مواطنيها ومن يقيم عليها خاضعة لحمايتها، وتُطبق أعلى المعايير في حفظ البيانات عليها.

٢. **حماية أمن الدولة بشكل عام:**وهذه الإيجابية المهمة (الأمن الوطني لكل دولة) مرتبطة بحماية معلومات الأفراد الخاصة، إذ إن الدولة عبارة عن أفراد يعيشون على أرض ضمن حدود معينة، فحماية بيانات الأفراد هي حماية للدولة نفسها في نهاية المطاف. واختراق معلومات الأفراد والتأثير عليها قد يكون من خارج الدولة، أي من دولة أخرى تكون لها أهداف وغايات تخدم مصالحها، وهي ضد الدولة مقر البيانات، وهذا فيه خطر كبير على الأمن الوطني. وأهم مثال يوضح ذلك، عملية التأثير السياسي التي قامت بها روسيا في انتخابات الولايات المتحدة الأمريكية عام ٢٠١٦م وعام ٢٠٢٠م، حيث كشفت أجهزة الاستخبارات الأمريكية وسلطات الأمن هناك العديد من المحاولات التي تقوم بها جماعات وأفراد تابعة للحكومة الروسية للتأثير على مسار الانتخابات الأمريكية، سواء أكان ذلك عبر الاختراق الإلكتروني لبيانات الأفراد أو

عبر التأثير من خلال حسابات التواصل الاجتماعي، حيث يحلل المخترقون البيانات الخاصة بعدد كبير من أفراد الشعب الأمريكي ثم يحاولون التأثير على آرائهم من خلال حسابات وهمية، وبالتالي التأثير على الانتخابات الأمريكية من خلال تلك الحسابات. وقد أصدر مكتب التحقيقات الفدرالي FBI بيانا يطلب فيه أمنيا عددا من الأفراد الروس الذين كشفت الأجهزة محاولاتهم تلك.[٢٧]ومثل ذلك يقال في العلاقة بين الصين وأمريكا حيث "تخوض الصين والولايات المتحدة حاليا حربا تجارية. في مثل هذه الحالة، إذا تم تخزين البيانات المتعلقة بالمواطنين الصينيين في خوادم موجودة في الولايات المتحدة، فمن المحتمل أن تكون هذه البيانات خاضعة للمراقبة الأجنبية"، ولذلك "استيقظت العديد من البلدان على تهديد المراقبة الأجنبية لقنوات المعلومات الخاصة بها، وبالتالي بدأت في المطالبة بتوطين البيانات".[٢٨]أما الجانب الاقتصادي فهو معتمد بشكل كبير على مقولة جديدة في عالم الأعمال مفادها أن (البيانات هي النفط الجديد). هذا يعني أن البيانات لها قيمة كبيرة جدا وإذا تم تحليلها بشكل صحيح يمكن أن تكون العمود الفقري لأي عمل تجاري ناجح.[٢٩]ومن هذا المنطلق فإن عددا من الدول تفرض توطين القوانين لتحقيق أهدف وإيجابيات اقتصادية مهمة، من أهمها:

١. **مصدر دخل للدولة ودعم لاقتصادها:**من المعلوم أن شركات التقنية الكبرى،وبالذات شركات التواصل الاجتماعي تحقق قيما مالية عالية جدا وذلك لما تستحوذ عليه من معلومات وبيانات شخصية متعلقة بالأفراد على مستوى العالم، فمثلا قيمة شركة meta المالكة لفيسبوك وواتساب وإنستغرام بلغت في عام ٢٠٢٢م ما يزيد على ٣٠٠ مليار دولار،[٣٠] كما بلغت قيمة شركة تويترفي صفقة استحواذإيلون ماسك عليها ٤٤ مليار دولار،[٣١] وهذه القيم العالية تعتمدبشكل كبيرعلى البيانات التي تستحوذ عليها الشركة بشكل مجاني من المستخدمين على مستوى العالم. ومن هنا تحفزت الدول للحصول على ضرائب من هذه الأرباح التي تحققها الشركات التي تعتمد على معلومات الأفراد المنتمين لهذه الدول. ولهذا "يعتقد أنصار توطين البيانات أنه يجب اعتبار البيانات موردا وطنيا.وهذا يعني أن الحكومة يجب أن يكون لها الحق في الإيرادات المتولدة من هذا المورد. تماما كما يتم فرض ضرائب على تدفق السلع والخدمات إلى الداخل وإلى الخارج، يجب أيضا فرض ضرائب على حركة البيانات داخل وخارج الدولة".[٣٢] وهذا الهدف له وجاهة،فكيف يمكن لهذه الشركات الكبرى أن تحقق ثروات هائلة من خلال بيانات ومعلومات تعود في الأصل لمواطنين وأفراد لا ينتمون لها، فمن حق الدول أن تستفيد أيضا من خلال فرض الضرائب على استخدام معلومات مواطنيها.

٢. **دعم الشركات المحلية لمنافسة الشركات العالمية:**وهذا الهدف مهم جدا للدول النامية والتي تريد أن تدعم العمل التقني والرقمي فيها، فمع تضخم الشركات الكبرى وسيطرتها واحتكارها للعالم الرقمي، لا يمكن للشركات المحلية الناشئة أن تنمو وتنافس دون دعم الدول لها، ولهذا "فإن الحكومات التي تفرض توطين البيانات تود إعطاء ميزة تنافسية لشركاتها المحلية، حيث تمنع الحكومة تدفق البيانات إلى الدول الخارجية. وبالتالي، ستكون البيانات متاحة للاستخدام الداخلي من قبل الشركات المحلية. وسيؤدي هذا إلى إنشاء "عدم تناسق في المعلومات" information asymmetry والذي سيصبح مناسبا للشركات المحلية."[٣٣]والمقصود بعدم التناسق في المعلومات information asymmetry أو عدم تناسق المعلومات، هو وجود معلومات وبيانات لطرف أكثر من الطرف الآخر، وهذا يعطي ميزة تنافسية للذي يملك معلومات أكثر ويصبح أكثر قدرة على التفوق والاستثمار والمخاطرة،[٣٤] وفي هذا السياق وفي حال فرض توطين البيانات يكون للشركات المحلية تنافسية أكثر من الشركات الدولية.

٣. **دعم اقتصادات جديدة:**توطين البيانات وتخزينها في البلد، بالإضافة إلى كونه يحقق مداخيل جيدة للبلد نفسه سواء للقطاع العام أو الخاص، فهو كذلك يولد اقتصادات جديدة وينشئ دوائر اقتصادية حديثة تدعم الاقتصاد بشكل عام. فمثلا توطين البيانات يستلزم إنشاء مراكز تخزين البيانات، وهذا يعني أنه لا بد من إنشاء شركات تقوم ببناء هذه المراكز التي تتطلب أجهزة ذات أحجام كبيرة، وتقنية معقدة. كما تتطلب عناية خاصة، ما يستلزم متخصصين ذوي معرفة عالية ومهنية ودقيقة، ما يعني أنه لا بد من نقل المعرفة إلى البلد ومن ثم تدريب عدد كبير من المختصين لتركيب وصيانة هذه الأجهزة المعقدة التي ستكون تحت الاستخدام على مدار ٢٤ ساعة. بالإضافة إلى ذلك، فإن هذه المراكز تتطلب مساحات كبيرة، أي إن قطاع العقار سينتعش ويولد نوعا جدا من الاستثمار العقاري الذي سيكون جديدا على البلد. ومن جانب آخر، فإن هذه البيانات تحتاج إلى حماية سيبرانية من أي اختراق داخلي أو خارجي، ولهذا لا بد من إنشاء شركات متخصصة في الأمن السيبراني، وتدريب فريق متخصص، والذي سيكون تحت العمل على مدار الساعة؛ لحماية الأمن السيبراني الذي يعد أمنا وطنيا للبلد بشكل عام.هذه بعض الأمثلة التي توضح كيف أن في فرض توطين البيانات فوائد اقتصادية كبيرة، ولو لم يُفرض التوطين، فإن هذه الاقتصادات الجديدة قد لا تنشأ في البلد، ما يفوت عليه فرصة نمو اقتصادي مهمة وتنافسية وحديثة.

المطلب الثاني: السلبيات المترتبة على توطين البيانات

السلبيات في فرض توطين البيانات عديدة ومتنوعة أيضا، وتختلف وجهات النظر حولها، ويمكن إبراز أهمها في جانبين، اقتصادي وسياسي، أما الاقتصادي:

١. **نهاية زمن الإنترنت:** تزعم شركات التقنية الكبرى أن في فرض توطين البيانات نهاية لزمن الإنترنت وما حققه من ثورات اقتصادية هائلة حيث "يقوم الإنترنت على مبدأ حرية حركة البيانات، وإذا أُعيقت هذه الحركة الحرة بفرض الضرائب أو بفرض توطين البيانات، فسوف ينتهي الأمر بتدمير الإنترنت. والسبب وراء تفضيل العديد من الشركات للإنترنت أنه أرخص وخالٍ من التنظيم المفرط. وإذا أجرت الحكومات أي تغييرات على النظام الحالي، فقد ينتهي بها الأمر بقتل التكنولوجيا الأكثر ثورية التي أنتجها العالم على الإطلاق".[٣٥] وبالتالي، فإن توطين البيانات يؤثر بشكل كبير – على حسب قول شركات التقنية الكبرى – على قابلية الاختراع والتطور السريع في هذه الصناعة في حال فرض توطين البنات في العالم.هذه المقولة "نهاية زمن الإنترنت" يرددها الكثير من شركات التنقية في معارضتهم لتوطين البيانات، والذي أراه أن فيها مبالغة بهذا الخصوص، فتوطين البيانات ليس المقصود منه المنع من تنقلها وحركتها، بل هو إلزام الشركات بحفظها في أراضي الدولة بدلا من حفظها في مكان آخر، وبالتطور التكنولوجي الهائل، لا يحد هذا من سرعة تنقل المعلومات ولا يحد من حريتها، أما فرض الضرائب، فهو موجود في جميع أنواع التجارات والأعمال ولم يطالب أحد بإلغاء الضرائب دعما للتجارة الحرة، فما الذي يمنع من فرضها أيضا على البيانات، والتي تشكل نفط العصر الجديد كما يقول ذلك أصحاب الشركات التقنية نفسها.

٢. **التأثير سلبا على النمو الاقتصادي للدول:** وهذا الأثر مرتبط بالذي قبله، فمناهضو توطين البيانات يزعمون أن في فرض توطين البيانات والحد من حركتها أثر سلبي كبير على نمو اقتصادات الدول، وبالذات الدول النامية، حيث تعتمد شركاتها بشكل كبير على البيانات التي تأتي من خارج الدولة وبكل سهولة، وفي الحد من ذلك حد من نموها وتطورها. ولهذا، نجد إحدى الدراسات التي توقعت أن الهند مثلا عند فرضها توطين البيانات "قد تتكبد ما يقرب من واحد (١) في المائة خسارة في الناتج المحلي الإجمالي (GDP) في المدى القصير والمتوسط إذا مضت الدولة قدما في توطين البيانات الإجباري في شكلها الحالي. علاوة على ذلك، إلى جانب التأثيرات على الناتج المحلي الإجمالي (المذكورة أعلاه) وجدت دراسة أجراها المركز الأوروبي للاقتصاد السياسي الدولي أن توطين البيانات سيضرب النمو المتوقع في الهند بنسبة ٢٠٪."[٣٦]، و"ستكون الشركات الناشئة هي الأكثر تضررًا حيث سيكلف إنشاء وتشغيل الأعمال التجارية أكثر نظرا لأن الشركات الناشئة قد لا تتمكن من تخزين البيانات على بدائل أرخص (مثل البنية التحتية السحابية) إذا تم إجبار جميع البيانات على أن تخزّن داخل الهند".[٣٧]وسبب التركيز على الهند وحرص شركات التقنية الكبرى على معارضة توطين البيانات فيها، أمران: الأول: أن الهند تعد من أكبر الدول في الصناعة الرقمية، وذلك بسبب التعليم التقني الجيد لديها وقلة تكلفة الأيدي العاملة هناك، ولهذا فكثير من الشركات التقنية تتواجد في أمريكا مثلا أو أوروبا، لكنها تتعاقد مع شركات هندية أو أفراد هنود يعيشون في الهند للقيام بعمليات البرمجة وغيرها من الخدمات التقنية والرقمية (outsourcing). والسبب الثاني: أن الهند في صدد فرض قانون يجبر الشركات على توطين البيانات الخاصة بمواطنيها داخل الهند، ولذلك نشأت ردة فعل كبيرة من الشركات التقنية الكبيرة تجاه هذا القانون وصدرت العديد من الدراسات التي تحذر الحكومة الهندية من فرض القانون، وتزعم تلك الدراسات أن القانون يؤثر بشكل سلبي على اقتصادات شركات التقنية الهندية والتي تقوم على تقديم الخدمات للشركات العالمية الكبرى والمبنية بشكل كبير على حركة البيانات السلسة بين الهند والعالم.[٣٨]هناك عدد من الثغرات في هذه السلبيات التي تُضعف قوتها وحجّيتها، أولا: أنها ما زالت فرضيات بعد وليست حقائق؛ حيث لم تطبق قوانين توطين البيانات بشكل فعلي حتى الآن في أغلب دول العالم. ثانيا: أنها أغفلت جوانب اقتصادية أخرى قد تكون نتائجها إيجابية جدا تطغى على هذه السلبيات، كما وضحنا ذلك أعلاه. ثالثا – وهو الأهم –: أن توطين البيانات لا يعني أبدا الحد من حريتها وسلاستها (كما وضحنا ذلك سابقا)، بل هو إجبار للشركات على تخزين البيانات في الدولة نفسها وليس خارجها، وكما ذكرنا ذلك سابقا، وبسبب التطور التقني الهائل، فإن هذا لا يحدّ من سرعة البيانات ولا من حركتها، وبالتالي فجميع المخاوف الناشئة من الحد من حركة البيانات وسلاسة مرورها بين الدول ليس له مبررات. أما السلبيات السياسية الذي يذكرها منتقدو توطين البيانات، فمن أهمها:

١. **زيادة سيطرة الدول على مواطنيها:** حيث يقول منتقدو توطين البيانات: "لا يحرص مواطنو العديد من الدول على منح حكوماتهم القدرة على التجسس عليهم. إذا تم تخزين جميع البيانات داخل الحدود الجغرافية، فستتمكن الحكومات من تجميع جميع البيانات وانتهاك خصوصية الأفراد إذا لزم الأمر."[٣٩]ولتوضيح هذا الأمر، إذا كانت البيانات تدار من شركة تقنية مثل تويتر، وهذه البيانات مخزنة في مركز تخزين بيانات موجود في أوروبا، ولنفترض أن هذه البيانات تخص مواطنا ينتمي لدولة أفريقية، ثم طلبت هذه الدولة بيانات هذا المواطن من الشركة الأمريكية، فوفقا للقانون الدولي، هذه الشركة لا تخضع لأي اختصاص قانوني للدولة الأفريقية، بل حتى مركز تخزين البيانات موجود في دولة أخرى، وبالتالي

لا تستطيع الدولة الأفريقية أن توجه أمرها كذلك للشركة التي تدير تخزين البيانات، بينما لو كان مركز تخزين البيانات موجود داخل هذه الدولة، فهو إذا خاضع لقوانينها وأنظمتها وملتزم بالأوامر والتوجيهات الصادرة من السلطات المختصة في تلك الدولة. ولهذا فالشركات تركز على أنه بما أن دول العالم الثالث ليست متقدمة في مجال حقوق الإنسان، فهي ترفض بناء مراكز بيانات فيها حتى لا تخضع لمثل هذه القوانين لو طلبت تلك الدول معلومات خاصة بأحد مواطنيها لسبب مخالف لحقوق الإنسان. وهذه السلبية تقودنا للسلبية الأخرى، وهي:

٢. **تقييد الحريات ومناهضة الديمقراطية:**يقول معارضو توطين البيانات: "لقد أدى جمع البيانات الشخصية إلى كسر مفاهيم الخصوصية، حيث تتجه مجموعة من الدول نحو الاستبداد الرقمي من خلال تبني النموذج الصيني للرقابة المكثفة وأنظمة المراقبة الآلية. ونتيجة لهذه الاتجاهات، تراجعت حرية الإنترنت العالمية... كما يمكن استخدام الإنترنت لتعطيل الديمقراطيات بقدر ما يمكن بالتأكيد زعزعة استقرار الأنظمة الديكتاتورية".[٤٠] فمن خلال تخزين البيانات في الدولة نفسها – حسب ما يقوله معارضو توطين البيانات – سيساعد هذا الدولة ليس في طلب المعلومة إذا أرادت الوصول إليها فحسب، بل سيمكنها كذلك من متابعة بيانات المواطنين ومراقبتها من خلال أجهزة الذكاء الاصطناعي التي قد تتنبأ بحدوث أي زعزعة أو مظاهرة أمنية قبل وقوعها، وبالتالي ستمكن الأجهزة الأمنية من عمل إجراءات استباقية قبل وقوع هذه الأحداث، وهي الإجراءات لا يمكن تحققها لولا وجود هذه البيانات وتخزينها في البلد نفسه، وبالتالي فإنه "يمكن لقوانين توطين البيانات الصارمة أن تمكّن من الاضطهاد السياسي من خلال إخضاع المعلومات للسيطرة الحكومية وتهديد الحقوق الفردية مثل حقوق الخصوصية وحماية البيانات ومناهضة التمييز وحرية التعبير، والقيم الديمقراطية".[٤١]لكن هذه السلبيات السياسية المطروحة يمكن مناقشتها من جانبين مهمين: أولا: أن موضوع الأمن الوطني موضوع سيادي يخص كل دولة وسيادتها على أرضها وشعبها، ولا يحق لأي دولة أخرى – فضلا عن الشركات العالمية – أن تتدخل في هذه الأمور الخاصة والحساسة، فلا يحق للشركات العالمية أن تطالب بأمور أو تمتنع عن أمور تخل بمبدأ السيادة، وهذا مبدأ واضح ولا إشكال فيه.

والجانب الثاني – وهو الأهم –: أنه حتى الولايات المتحدة الأمريكية التي تنتمي لها أغلب الشركات التقنية الكبرى، لديها مثل هذا النوع من القوانين ويحق لها أن تطلب معلومات خاصة إذا كان ذلك متعلقا بالأمن الوطني، حيث إن مكتب التحقيقات الفيدرالي يحق له أن يطلب بموجب "خطاب أمن قومي" The National Security Letter (NSL) بناء على قانون The Patriot Actطلب سجلات العملاء الشخصية من مزودي خدمة الإنترنت ومن المؤسسات المالية ومن شركات الائتمان دون موافقة مسبقة من المحكمة"[٤٢] فمن خلال خطاب الأمن القومي (NSL)، "يمكن لمكتب التحقيقات الفيدرالي (FBI) تجميع ملفات ضخمة حول الأشخاص الأبرياء والحصول على معلومات حساسة مثل مواقع الإنترنت التي يزورها الشخص، أو قائمة بعناوين البريد الإلكتروني التي تراسل معها الشخص، أو حتى كشف هوية الشخص الذي نشر خطابا مجهولا على موقع سياسي. كما يُسمح له أيضا بمنع أي شخص يتلقى خطاب الأمن القومي من إخبار أحد بذلك".[٤٣]فإذا كان هذا مسموحا به بل ومعمولا به في الولايات المتحدة الأمريكية مع هذه الشركات التقنية الكبرى وغيرها، فلماذا تتذرع تلك الشركات بما يخالف ذلك في عدم تخزين البيانات في غيرها من الدول. فما يحق للولايات المتحدة الأمريكية من طلب معلومات خاصة بقصد الأمن القومي، يحق لغيرها من الدول كذلك.الخلاصة: أنه إذا نظرنا لمصلحة الدول وشعوبها، لا سيما الدول النامية، فإن الإيجابيات الاقتصادية والأمنية ترجح على السلبيات من وجهة نظر الباحث، بل إن السلبيات المذكورة غالبها تنادي بها شركات التقنية الكبرى؛ لأن في توطين البيانات حد من مصالحها بشكل مباشر، سواء أكانت مصالح مالية وهي الأهم، أم مصالح لوجستية وعملية. وبالتالي فشركات التقنية الكبرى هي المتضرر الأكبر من توطين البيانات، وليس غيرها. ولهذا، فكثير من الدول ماضية قدما في توطين البيانات – رغم النداءات والاصوات المعارضة – على اختلاف مناهجها وطرائقها، كما سيتضح ذلك في المبحث القادم، بإذن الله تعالى.

المبحث الثالث: الاتجاهات الدولية التشريعية في توطين البيانات، وموقف الدول العربية من ذلك

المطلب الأول: الاتجاهات الدولية في توطين البيانات

سبق أن ذكرنا في المبحث الأول أن ثمة نوعا من البيانات لا خلاف بين الدول في وجوب حفظها وتخزينها في الدولة نفسها وعدم خروجها من أراضيها، وذلك مثل البيانات العسكرية والأمنية، وغيرها من البيانات الحساسة المتعلقة بالأمن الوطني، والخلاف يقع في غيرها من البيانات، والتي هي على وجه الخصوص ما له علاقة بالبيانات الشخصية، حيث اختلفت مسارات الدول فيها إلى ثلاثة اتجاهات، وهذا ما سيُبحث ويُوضّح في هذا المبحث.

الاتجاه الأول: وجوب توطين البيانات، وتخزينها، وحفظها، في البلد نفسه

هذا التوجه يُلزم الشركات الخاصة التي تتعامل مع البيانات الشخصية لمواطني الدولة والمقيمين فيها بوجوب تخزين البيانات ومعالجتها في الدولة نفسها. وعلى رأس هذا التوجه روسيا والصين، حيث ينص القانون الفيدرالي الروسي رقم ٢٤٢-fz – الذي دخل حيز التنفيذ في سبتمبر ٢٠١٥م – على أن "مشغلي البيانات الروس والأجانب الذين يجمعون البيانات الشخصية للمواطنين الروس ويقومون بتسجيلها وترتيبها وتجميعها وتخزينها وتحديثها وتعديلها واسترجاعها يجب عليهم استخدام خوادم في الاتحاد الروسي".[٤٤]ومثلها في الإلزام: الصين، ولكن بنصوص قانونية أقل صرامة، حيث نص قانون الأمن السيبراني الصيني، التي دخل حيز التنفيذ في يونيو ٢٠١٧م على وجوب توطين البيانات الشخصية و "البيانات المهمة" (البيانات التي تثير الأمن القومي أو الحساسيات الاستراتيجية للحكومة الصينية، مثل البيانات الحكومية غير المنشورة أو البيانات الجغرافية أو البيانات المتعلقة بالصناعات الحساسة / الاستراتيجية)، ولكن هذا الإلزام خاص بالمنظمات المصنفة كـ "مشغلي البنية التحتية للمعلومات الحيوية"، والتي تعني بشكل عام، أنظمة وشبكات واسعة النطاق مملوكة للدولة والقطاع الخاص ذات أهمية حساسة للصين."[٤٥]ثم بعد ذلك صدر قانون حماية المعلومات الشخصية والذي دخل حيز التنفيذ في نوفمبر ٢٠٢١م، وهذا القانون أكّد الحكم الوارد في قانون الأمن السيبراني، ثم وسّع النطاق ليشمل جميع المعلومات الشخصية للمواطن الصيني، وأنه لا يجوز إخراج البيانات الشخصية لأي مواطن صيني إلا بشروط، أهم هذه الشروط هي موافقة الشخص صاحب العلاقة موافقة صريحة على نقل هذه البيانات، ولا بد كذلك من موافقة إدارة الأمن السيبراني الصينية؛ للتأكد من أن المكان الذي ستنتقل إليه المعلومات موافق للمعايير والشروط الصينية. هذه الموافقة لا بد أن تكون صريحة، وتَصدر شهادة من إدارة الأمن السيبراني بذلك، وهنا يأتي تدخل الحكومة الصينية، إذ إن الواقع العملي أن إدارة الأمن السيبراني الصينية لا توافق على نقل هذه المعلومات.[٤٦]وروسيا والصين ليستا الدولتين الوحيدتين في هذا الاتجاه، "فقد طلبت نيجيريا أن تكون جميع بيانات المشتركين والمستهلكين في شركات تكنولوجيا المعلومات والاتصالات مخزنة محليا داخل البلاد وكذلك البيانات الحكومية، وهذا القرار صادر منذ ديسمبر ٢٠١٣م، وتُلزم ألمانيا شركات الاتصالات ومقدمي خدمات الإنترنت بتخزين البيانات داخل أراضيها.وثمة قوانين في أستراليا وكولومبيا البريطانية ونوفا سكوشا الكندية والهند تقيد تصدير البيانات داخل قطاعات معينة، مثل الصحة والحوكمة المحلية".[٤٧]ولكن الذي يميز روسيا والصين هو شمولية توطين البيانات، وأنه لا يجوز إخراج هذه البيانات – أيا كانت هذه البيانات – خارج الحدود الجغرافية إلا باستثناءات خاصة نص عليها القانون.ويلحظ في هذا التوجه تزعّم الصين وروسيا وتبنيهما له، ولا يمكن فصل ذلك عن الصراع السياسي القائم حاليا بين الشرق (وتمثله الصين وروسيا) والغرب عامة، وبالأخص الولايات المتحدة الأمريكية، فهذا الصراع له جوانب عديدة: سياسية، واقتصادية، ومالية، وعسكرية، وتكنولوجية، وفضائية... وغيرها. ومن جوانب هذا الصراع: البيانات والسيطرة عليها والتحكم فيها، فالبيانات يقال عنها حاليا إنها "نفط العصر"، كما ذكرنا ذلك سابقا. لا سيما أن شركات التقنية الكبرى ما زالت في أغلبها أمريكية، وهي خاضعة بشكل أو بآخر للقوانين الفيدرالية الأمريكية.من أجل ذلك تزعّمت روسيا والصين توطين البيانات من باب السيادة الوطنية، وكذلك من باب الاستقلال عن الهيمنة الأمريكية، فضلا عما يحققه ذلك من إيجابيات أخرى ذكرنا بعضا منها سابقا.

الاتجاه الثاني: لا يشترط التوطين، ولكن بشروط

ويتزعم هذاالتوجه الاتحادالأوروبي من خلال قانونه المسمى القانون العام لحماية البيانات" General Data Protection Regulation والمعروف اختصارا بـ (GDPR). هذا القانون (GDPR) دخل حيز التنفيذ عام ٢٠١٨م،بعداعتماده من المفوضية الأوروبية،وأصبح ملزما لجميع الدول التابعة للاتحاد الأوربي،ويعد هذا القانون نقلة وتحولاجوهريافي التعامل مع البيانات الشخصية. فبعد أن كانت شركات التقنية تسرح وتمرح في الاستفادة من البيانات الشخصية لجميع الأفراد في العالم، جاء هذا القانون ليضع حدا كبيرا لهذه الحرية، حيث إن القانون يُطبق على الشركات الموجودة في الاتحاد الأوروبي، ويُطبق كذلك على الشركات التي تعمل خارج الاتحاد الأوروبي؛ لكنها تتعامل مع بيانات مواطنين ومقيمين في الاتحاد الأوروبي. وصار هذا القانون نموذجا لدول العالم بعد ذلك بل حتى إن الدول التي تتبنى الاتجاه الأول، مثل روسيا والصين، استفادت كثيرا من القانون الأوروبي، وأضافت عليه اشتراطات تخدم توجه الدول نفسها، لهذا فإن GDPR يعد النقلة الحقيقية والتغيير الجوهري في التعامل مع بيانات الأفراد عالميا.[٤٨]هذا القانون طويل ومفصل ودقيق، حيث يحتوي على أحد عشر فصلا، وما يقارب ١٠٠ مادة[٤٩]، والذي يهمنا منها هو موقف قانون GDPR من نقل البيانات خارج الاتحاد الأوروبي فالقانون يسمح بتحرك البيانات بكل حرية داخل حدود الاتحاد الأوربي؛ ولكن يمنع نقلها خارجه إلا في حالات معينة، يعد توفّر أحدها كافيا للسماح بنقل البيانات خارجه، وهذه الحالات هي كما يلي[٥٠]:

أولا: إذا كان البلد الذي ستنتقل إليه البيانات من البلدان المعتمدة لدى الاتحاد الأوروبي لنقل البيانات، وقائمة الدول المعتمدة تخضع للتحديث الدوري من قبل المفوضية الأوروبية، وتسمى دول الكفاية Adequacy countries، بمعنى أن هذه الدول بعد تقييم المفوضية لها، لديها

معايير كافية لحماية البيانات. وحسب آخر تحديث فقد "اعترفت المفوضية الأوروبية حتى الآن بأندورا، والأرجنتين، وكندا (منظمات تجارية)، وجزر فارو، وغيرنسي، وإسرائيل، وجزيرة مان، واليابان، وجيرسي، ونيوزيلندا، وجمهورية كوريا، وسويسرا، والمملكة المتحدة، وأوروغواي؛ بموجب القانون العام لحماية البيانات (GDPR)، باعتبار هذه الدولة توفر الحماية الكافية."[٥١] وبالتالي، فإن نقل البيانات خارج الاتحاد الأوروبي لإحدى هذه الدول يعد مسموحا به، وفقا لـ GDPR بدون شروط.

ثانيا: أن يكون المرسل والمتلقي ضمن شركتين منفصلتين ويلتزمان بعقد يحتوي على بنودقياسية لحماية البيانات، هذه البنودمحدد ومفصلة في الـGDPR.

ثالثا: أن يكون المرسل والمتلقي ضمن كيانات مختلفة لشركة متعددة الجنسيات، مثل: آبل Apple، ومايكروسوفت Microsoft، وأمازون Amazon، وجوجل Google ، وغيرها. والتي لها فروع كثيرة في الاتحاد الأوروبي ولكن مقرها الرئيس خارجه، ولهذه الشركة معايير وقواعد قياسية لحماية البيانات وموافقة لمعايير قانون GDPR (أو قد تكون أعلى منها)، ويتناقل الموظفون في هذه الشركات البيانات خارج الاتحاد الأوروبي، وفي هذه الحالة يكون نقل البيانات مسموحا به، نظرا لوجود هذه المعايير.

رابعا: إذا تم نقل البيانات وفقا لأحد الاستثناءات الواردة في قانون GDPR، وقد نصت المادة ٤٩ منه على هذه الاستثناءات، ومن تلك الاستثناءات ما يلي:

١. "أن يوافق الشخص الذي يتم نقل بياناته على وجه التحديد، بعد إبلاغه بالمخاطر.
٢. أن يكون النقل ضروريا في سياق دعوى قانونية.
٣. أن يكون النقل ضروريا لأسباب مهمة تتعلق بالمصلحة العامة.
٤. أن يكون النقل ضروريا لإنقاذ حياة الشخص، بعد تعذر الحصول على موافقته".[٥٢]

والفرق بين الحالة الرابعة والحالات الثلاث التي قبلها، أن الحالة الرابعة استثنائية، أي تحصل لمرة واحدة، ولموقف واحد، ولا يتكرر. بينما تشكّل الحالات السابقة الإطار الذي يسمح بتدفق البيانات وتحركها بشكل كامل دون الرجوع إلى الجهة المختصة في كل مرة.[٥٣]ما ذكر أعلاه يعطي تصورا عن مستوى التفاصيل والجزئيات التي تحدث عنها قانون GDPRفي موضوع واحد فقط، وهو توطين البيانات ونقلها، ورغم أن القارئ قد يرى فيه نوعا من التسامح مقارنة بالاتجاه الأول الذي منع نقل البيانات خارج الحدود الجغرافية مطلقا، إلا أنه إذا قارناه بموقف السوق العالمي للبيانات قبل عام ٢٠١٨م (وقت إقراره) وبموقف الولايات المتحدة الأمريكية، الدولة الرائدة في هذه المجال، يدرك القارئ النقلة النوعية التي أحدثها هذا القانون، وهو ما سيتضح من خلال دراسة الاتجاه الثالث.

الاتجاه الثالث: عدم اشتراط توطين البيانات

ويتزعم هذه الاتجاه الولايات المتحدة الأمريكية التي تدعو إلى حرية تدفق المعلومات وتنقلها بين الدول (المقصود بالمعلومات هنا التي ليس لها علاقة بالأمن القومي ولا بالمعلومات العسكرية والحكومية الحساسة، كما سبق توضيح ذلك في تعريف توطين البيانات) لما في ذلك من دعم للاقتصاد العالمي ونمو لشركات التقنية. ولهذا لا يوجد قانون فيدرالي أمريكي يجبر الشركات على توطين البيانات في الولايات المتحدة الأمريكية، بل لا يوجد أصلا قانون فيدرالي ينظم خصوصية البيانات الخاصة للأفراد مطلقا، والموجود عبارة عن معايير في السوق تلتزم بها الشركات من باب حماية سمعة الشركة، وليس من باب الإلزام القانوني. وهناك بعض القوانين التي تنظم اختراق البيانات وبعض المسائل الخاصة، ولكن على مستوى الولايات، وليس على مستوى الحكومة الفيدرالية، ولكن لا يوجد قانون عام، كما هو موجود في الاتحاد الأوروبي، ينظم حماية البيانات الخاصة ويُلزم بتوطينها في الولايات المتحدة الأمريكية. [٥٤] والولايات المتحدة الأمريكية ذهبت في هذا الباب إلى أبعد من ذلك، حيث وقّعت كل من الولايات المتحدة والمكسيك وكندا اتفاقية "دخلت حيز التنفيذ في يوليو ٢٠٢٠م واستبدلت اتفاقية التجارة الحرة لأمريكا الشمالية، تحظر فيها توطين البيانات وتضفي الطابع الرسمي على التدفق الحر للبيانات بين الدول الأعضاء"[٥٥]، وهذا من مبدأ أن "الاتفاقيات التجارية المتعددة بين الدول الديمقراطية في المنطقة تحظر كلا من متطلبات توطين البيانات، وقيود تدفق البيانات عبر الحدود."[٥٦]فالولايات المتحدة الأمريكية لا تلزم بتوطين البيانات فحسب، بل تمنع وتدعو الدول الديمقراطية كذلك إلى منعه، وترى أن تدفق المعلومات مثل تدفق البضائع والسلع، كل ما كان سهلا، زاد ذلك في نمو الاقتصاد العالمي.ولكن على القارئ الكريم أن يعلم أيضا أن الولايات المتحدة الأمريكية أصدرت قانونا فيدراليا في عام ٢٠١٨م اسمه "توضيح الاستخدام القانوني للبيانات في الخارج" Clarifying Lawful Overseas Use of Data Act أو ما يعرف اختصارا بـ"قانون كلاود" Cloud Act، فمع تطور شركات التقنية وكبر حجم البيانات عالميا، وحيث إن أغلب شركات

التقنية الكبرى هي شركات أمريكية في الأساس، مثل مايكروسوفت Microsoft، وجوجل Google ، وآبل Apple ، وفيسبوك Facebook ، وأمازونAmazon ، وتويتر Twitter ، وهذه الشركات الأمريكية قد تحتفظ ببياناتها خارج الولايات المتحدة الأمريكية، فإن هذا القانون يمكّن الحكومة الفيدرالية الأمريكية من "إجبار شركات التقنية الأمريكية على تسليم البيانات الموجودة خارج الولايات المتحد،. حيث يتناول القانون ذلك من خلال السماح للحكومة الأمريكية بالحصول على بيانات المستخدم الواقعة ضمن حيازة أو وصاية أو سيطرة الشركة بغض النظر عن مكان الاحتفاظ بالبيانات".[٥٧]بل إن هذا القانون يعالج موضوعا أبعد من ذلك، حيث يمنع القانون الشركات الأمريكية التي لها فروع في الخارج أو مراكز تخزين بيانات في الخارج "من الاستجابة المباشرة لجهات إنفاذ القانون الأجنبية عندما تطلب بشكل قانوني بيانات مستخدم ما لأغراض التحقيق، إذا كان طلبها مخالفا للقانون الأمريكي"[٥٨]، ولا يسمح القانون بإعطاء الدولة الأجنبية هذه البيانات (حتى لو كان مركز البيانات على أراضيها) إلا إذا كانت هناك اتفاقية بين الولايات المتحدة الأمريكية وبين تلك الدولة.[٥٩] هذا القانون يفسر موقف الولايات المتحدة الأمريكية الداعم لتدفق البيانات وعدم توطينها، إذ إن الحكومة الأمريكية هي المستفيد الأكبر من ذلك أمنيا واقتصاديافمن الناحية الأمنية؛ لأن البيانات التي في حوزة الشركات الأمريكية (أيا كان محلها)؛ ولأن الشركات الأمريكية هي المسيطر الأكبر على بيانات الأفراد في العالم، فإن الحكومة الأمريكية تستطيع الحصول عليها وإجبار الشركات الأمريكية على تزويد الحكومة بها، وفقا لشروط ومتطلبات قانون كلاود. وفي المقابل، فإن الحكومات الأخرى ممنوعة من الحصول على تلك البيانات حتى لو كان مركز حفظها داخل أراضيهاأما من الناحية الاقتصادية؛ فإن تدفق البيانات ينمي الشركات الأمريكية الكبرى ماليا، وبالتالي يزداد دخل الحكومة الفيدرالية الأمريكية من خلال الضرائب التي تفرضها على هذه الشركات. بينما لا تحظى الحكومات الأخرى بهذه الامتيازات، لا الاقتصادية منها ولا الأمنية، مع أن الشركات الأمريكية تستفيد من بيانات مواطني تلك الدول بشكل مجاني. ولهذا وجدت الدول الداعمة لتوطين البيانات مدخلا في الاستفادة من نمو هذه السوق والصناعة العالمية اقتصاديا وأمنيا؛ ولكن بطريقة مخالفة لطريقة الولايات المتحدة الأمريكية.

المطلب الثاني: موقف الدول العربية من توطين البيانات:

سنذكر هنا نموذجين فقط من الدول العربية، وهما: جمهورية مصر العربية، والمملكة العربية السعودية، وسبب اختيار هاتين الدولتين من بين الدول العربية عدة أسباب:

١. يصعب ذكر جميع الدول العربية في هذا البحث.
٢. كثير من الدول العربية لم تصدر قوانين أو أنظمة تنظم وتقنن توطين البيانات حتى الآن، وبالأخص ما يتعلق بالبيانات الشخصية.
٣. والسبب الأهم هو أن هاتين الدولتين من أعلى الدول العربية من حيث عدد للسكان، حيث بلغ عدد السكان في مصر – حسب ما هو منشور في إحصائيات البنك الدولي لعام ٢٠٢١م – ١٠٩ ملايين نسمة. أما المملكة العربية السعودية فقد بلغ عدد السكان فيها، وفقا للمصدر نفسه ٣٥ مليون نسمة[٦٠]. وبالتالي فإن التعرض للبيانات الشخصية من قبل الشركات العالمية سيكون كبيرا، ولهذا تأخذ تلك الشركات حذرها في التعامل مع هاتين الدولتين، وتركز عليهما كثيرا حتى لا تقع فيما هو مخالف للقانون.

جمهورية مصر العربية:يلحظ أن مصر تبنت الموقف الأوروبي، والذي يقف وسطا في توطين البيانات بين الموقف الذي يمنع بالكلية والموقف الذي يسمح بذلك، فقد نصّ قانون حماية البيانات الشخصية الصادر في عام ٢٠٢٠م في المادة ١٤ على أنه "يحظر إجراء عمليات نقل للبيانات الشخصية التي تم جمعها أو تجهيزها للمعالجة إلى دولة أجنبية أو تخزينها أو مشاركتها إلا بتوفر مستوى من الحماية لا يقل عن تلك المنصوص عليها في هذا القانون، وبترخيص أو تصريح من المركز. وتحدد اللائحة التنفيذية لهذا القانون السياسات والمعايير والضوابط والقواعد اللازمة لنقل أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود وحمايتها."[٦١]أي أن القانون المصري يسمح بنقل البيانات الشخصية إلى دول أخرى إذا كانت هذه الدول تطبق نفس المعايير التي يشترطها القانون المصري، وأحال تفاصيل ذلك إلى اللوائح، وهذا موافق للتوجه الأوروبي الذي يسمح بنقل البيانات إلى الدول التي تطبق معايير قانون GDPR، وأن هناك قائمة يعتمدها الاتحاد الأوروبي لتحديد الدول التي تطبق المعايير نفسها. رغم أن لوائح قانون حماية البيانات الشخصية المصري لم تصدر بعد؛ ولكن القانون تبنى المبدأ نفسه. ومن مواطن التشابه كذلك مع القانون الأوروبي، أن القانون المصري يسمح بنقل البيانات الشخصية إذا وافق الشخص الذي تتعلق به البيانات في حالات محددة تشبه الحالات التي نص عليها القانون الأوروبي، وهو ما ذكرته المادة ١٥ "استثناء من حكم المادة (١٤) من هذا القانون، يجوز في حالة الموافقة الصريحة للشخص المعني بالبيانات أو من ينوب عنه، نقل أو مشاركة أو تداول أو معالجة البيانات الشخصية إلى دولة ا يتوفر فيها مستوى الحماية المشار إليها في المادة السابقة، وذلك في الحالات التالية"[٦٢] ثم ذكرت المادة الحالات. وهذا موافق

للاتحاد الأوروبي في نقل البيانات لدول لا تطبق المعايير نفسها وفق حالات محددة. وبالتالي فإن توجه الحكومة المصرية موافق للتوجه الأوروبي من حيث المبدأ في توطين البيانات، وهو مختلف عن موقف المملكة العربية السعودية، كما سيتضح ذلك.

المملكة العربية السعودية:أصدرت المملكة العربية السعودية نظام حماية البيانات الشخصية في عام ٢٠٢١م، والذي تناول موضوع توطين البيانات، ومن خلال هذا النظام يلحظ أن المملكة العربية السعودية أكثر تحفظا من مصر (ومن الموقف الأوروبي) في توطين البيانات، وقد تكاد تكون أقرب إلى الصين في هذا المجال، حيث نص النظام على أنه "فيما عدا حالات الضرورة القصوى للمحافظة على حياة صاحب البيانات خارج المملكة أو مصالحه الحيوية أو الوقاية من عدوى مرضية أو فحصها أو معالجتها، لا يجوز لجهة التحكم نقل البيانات الشخصية إلى خارج المملكة أو الإفصاح عنها لجهة خارج المملكة إلا إذا كان ذلك تنفيذا لالتزام بموجب اتفاقية تكون المملكة طرفا فيه، أو لخدمة مصالح المملكة، أو لأغراض أخرى وفقاً لما تحدده اللوائح".[٦٣]أي أن حكومة المملكة تمنع نقل أي بيانات شخصية خارج المملكة، حتى لو كانت تلك الدول على المعايير نفسها التي يشترطها النظام، ولا يسمح بنقل البيانات إلا في حالات الضرورة القصوى فيما يخص صاحب البيانات مثل "المحافظة على حياة صاحب البيانات خارج المملكة أو مصالحه الحيوية أو الوقاية من عدوى مرضية أو فحصها أو معالجتها"، أو إذا كان هناك اتفاقية بين المملكة وتلك الدولة، أو لخدمة مصالح المملكة، أما عدا ذلك فلا يسمح بنقل البيانات حتى لو كان ذلك بموافقة صاحب البيانات؛ بل حتى في هذه الحالات الاستثنائية، هناك شروط لا بد من توفرها نص عليها النظام، وهي:

١. "ألا يترتب على النقل أو الإفصاح مساس بالأمن الوطني أو بمصالح المملكة الحيوية.
٢. أن تُقدّم ضمانات كافية للمحافظة على البيانات الشخصية التي سَيُجرى نقلها أو الإفصاح عنها وعلى سريتها، بحيث لا تقل معايير حماية البيانات الشخصية عن المعايير الواردة في النظام واللوائح.
٣. أن يقتصر النقل أو الإفصاح على الحد الأدنى من البيانات الشخصية الذي تدعو الحاجة إليه.
٤. موافقة الجهة المختصة على النقل أو الإفصاح وفقاً لما تحدده اللوائح".وعليه، فإن المملكة العربية السعودية تعد من الدول التي تشترط توطين البيانات كما هو موضح في التوجه الأول، وصاغت هذا الاشتراط قانونيا بطريقة مشابهة لصياغة الصين في ذلك (وليس مثل حدية النص الروسي)، ونظرا لصعوبة هذه الشروط على شركات التقنية الكبرى وقوتها فإن المرسوم الملكي الذي أصدر النظام أعطى في ديباجته مهلة سنة كاملة للشركات لتصحح أوضاعها، وتكون موافقة للنظام من تاريخ النفاذ، حيث إن النظام صدر في شهر ٩ من عام ٢٠٢١م ونصت المادة ٤٣ منه على أن يُعمل به بعد ٦ أشهر من نشره، أي أن نفاذه في شهر ٣ من عام ٢٠٢٢م، وبالتالي فالمهلة ستستمر للشركات إلى شهر ٣ من عام ٢٠٢٣م، ورغم طول هذه المهلة، إلا أنه نظرا لصعوبة تنفيذ توطين البيانات بالشكل الذي اشترطه النظام السعودي، أجّلت الحكومة السعودية تاريخ نفاذ النظام سنة كاملة، أي من شهر ٣ عام ٢٠٢٢م إلى شهر ٣ عام ٢٠٢٣م، بسبب الاعتراضات الكبيرة التي وردت من شركات التقنية، وفق تصريح الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)، وهي الجهة المخولة بتنفيذ النظام وتطبيقه وإصدار لوائحه؛ حيث صرحت بما يلي: "بناء على ما تلقته من مرئيات وملاحظات من الأفراد والجهات العامة والخاصة المحلية والعالمية على مشروع اللائحة التنفيذية لنظام حماية البيانات الشخصية أثناء مدة استطلاع مرئيات العموم، ولأجل تحقيق الأهداف التي من أجلها وضِع النظام، وبناءً على ما تم رفعه من توصيات من قبل سدايا، فقد قررت الجهات المختصة تأجيل العمل بالنظام إلى تاريخ ٢٥ / ٨ / ١٤٤٤هـ، لاتخاذ ما يلزم حيال هذه التوصيات."[٦٤] أي أن النفاذ حسب التصريح سيكون في شهر ٣ من عام ٢٠٢٣م، ثم هناك سنة مهلة حسب المرسوم الملكي (أي إلى شهر ٣ من عام ٢٠٢٤م) للشركات حتى تتوافق مع النظام، فأصبحت المدة للشركات تزيد على السنتين من تاريخ نشر النظام.جاء تصريح الهيئة في التعليق على اللائحة، أما النظام نفسه فهو باق كما هو، وبالتالي فمبدأ توطين البيانات التي تبنته الحكومة السعودية سيستمر، وما أجلت المملكة التطبيق إلا لإعطاء فرصة أكبر للشركات حتى تتوافق مع هذا الاشتراط.

الخاتمة: النتائج والتوصيات

من خلال ما سبق بحثه، يمكن أن نخلص إلى النتائج التالية:

١. إن العالم يعيش اليوم "ثورة بيانات"، فكما شهد العالم الثورة الصناعية، وثورة (com.)، فإن المرحلة الحالية هي ثورة بيانات، ولهذا فإن لها آثارا كبيرة حالية ومستقبلية في شتى الجوانب السياسية والاقتصادية والاجتماعية، كما كان للثورات السابقة أثر كبير ما زال باقيا حتى الآن.
٢. تعدّ البيانات نفط هذا العصر، ولهذا فهي مورد اقتصادي كبير، وحمايتها أيضا يشكل أمنا وطنيا وقوميا لأي دولة، ولهذا هي مكن قوة سياسية واقتصادية، فكما كانت الحروب تُشن في القرن الماضي من أجل النفط، فإن الصراعات الآن بين الدول العظمى في السيطرة على هذه البيانات.

٣. لأجل أهمية البيانات وخطورتها السياسية والاقتصادية، حدث الجدال والخلاف التشريعي والقانوني بين الدول حول مكان تخزينها وحفظها؛ لأن السيطرة عليها تعد سيطرة على مكن قوة عالمي.

٤. نظرا لأن أغلب الشركات التي ستستحوذ على البيانات هي شركات أمريكية، نجد أن الولايات المتحدة الأمريكية لا تمانع من حفظ البيانات وتخزينها في أي مكان في العالم؛ لأن هذه الشركات في نهاية الأمر خاضعة للقانون الأمريكي، وتدفع ضرائب للحكومة الأمريكية، فالحكومة الأمريكية مستفيدة سياسيا واقتصاديا من هذه الشركات، أيا كان محل تخزين بياناتها.

٥. في المقابل، أجبرت الصين وروسيا الشركات العالمية على تخزين بيانات مواطنيها في الدولة نفسها، حتى يكون للصين وروسيا سيطرة أمنية واقتصادية على هذه البيانات، وسار مسارها عدد من الدول، ومنها: المملكة العربية السعودية.

٦. وقف الاتحاد الأوربي موقفا وسطا بين السماح بالكلية وبين المنع بالكلية، وفقا لشروط معينة.

٧. وراء كل توجه أهداف سياسية واقتصادية تسعى كل دولة لتحقيقها، والذي يظهر أن الأفضل للدول النامية أن تشترط توطين البيانات على الشركات الأجنبية حتى تستفيد اقتصاديا وسياسيا من وجود البيانات لديها، وبالذات الدول العربية، بشروط وضوابط محددة، كما سيأتي ذلك في التوصيات

أما التوصيات الناتجة عن هذا البحث، فهي كما يلي:

١. الآثار الإيجابية والاقتصادية في توطين البيانات للدول النامية كبيرة، ولهذا على الدول العربية أن تبادر في فرض التوطين؛ للاستفادة من هذه الآثار واستغلال هذا المورد الاقتصادي الجديد. وقد تواجه الدول العربية مشكلة عدد السكان، فمثلا الصين فيها مليار نسمة، فمن الطبيعي أن يكون لها مركز تخزين بيانات خاص بها، نظرا لعدد السكان؛ لكن لا يمكن أن تشترط دولة كالكويت أو قطر أو البحرين أو الأردن تخزين بياناتها داخلها؛ لعدد السكان القليل جدا، ويمكن تقادي هذه المشكلة بإيجاد اتفاقيات بين الدول العربية، كما هو معمول به في الاتحاد الأوروبي، وبالتالي وجود مركز بيانات في أي دولة من هذه الدول التي من ضمن الاتفاقية يلبي اشتراط توطين البيانات.

٢. على الدول العربية المبادرة في صياغة التشريعات التي تنظم خصوصية البيانات وتوطينها، فكما رأينا في ثنايا البحث أن قليلا من الدول هي التي لديها هذا النوع من القوانين، مثل المملكة العربية السعودية ومصر والأردن، وحتى هذه القوانين لم تصدر لوائحها بعد، والجيد في الموضوع، أن الدول العربية لن تصنع العجلة من جديد، بل ستبدأ من حيث ما انتهت إليه الدول الأخرى، بعد تطوير وتعديل ما توصلت إليه بما يوافق مصالح الدول العربية.

٣. لا بد أن تدرك الدولة التي ستشترط توطين البيانات وتخزينها في الدولة نفسها، أنه سينشأ عن ذلك التزام كبير يتعلق بتوفير الأمن السيبراني لهذه البيانات، لحماية البيانات من الاختراق الداخلي والخارجي، وذلك مثل أي مورد اقتصادي وأمني على الدولة أن توفر الحماية له؛ لكن هذه الحماية تتطلب نوعا معينا من المهارة والاحترافية التي هي حديثة نوعا ما.

٤. ولذلك،على الدول التي ستتبنى توطين البيانات أن تستثمرفي تعليم وتدريب ونقل معرفة تخزين البيانات وحمايتها سيبرانيا من الناحية التقنية،وبناء مراكز تخزين البيانات وصيانتها وتشغليها من الناحية الهندسية، وهذا سيكلف وقتا وجهدا ليس بالقليل على الدول الجديدة في هذ المجال.

٥. على الدول كذلك دعم الأبحاث القانونية والتقنية في مجال توطين البيانات،وذلك لأن هذا المجال سريع التطوروالتغير،والتشريعات واللوائح فيه لا بدأن تواكب التغيرات السريعة فيه،ويكون تحديثها وفقا لتطورالصناعة الحاسوبية والتقنية والرقمية في هذا المجال.**وصلى الله على نبينا محمد.**

المراجع:

أولا: المراجع العربية:

- "سدايا" تعلن تأجيل العمل بنظام حماية البيانات الشخصية. وكالة الأنباء السعودية. (https://www.spa.gov.sa/2339723).
- ضوابط الأمن السيبراني للأنظمة الحساسة. الهيئة الوطنية للأمن السيبراني. المملكة العربية السعودية. (https://nca.gov.sa/legislation?item=177&slug=controls-list).
- العتيبي، عبد الله بن جبر. (٢٠٠٩). العولمة وسيادة الدولة الوطنية: بحث في أهمية مفهوم السيادة في نظرية العلاقات الدولية. المجلة العربية للعلوم السياسية. عدد ٢٣. ص ص ٧١- ١١٢.
- عمران، ماجد؛ وكلثوم، فيصل. (٢٠١١). السيادة في ظل الحماية الدولية لحقوق الإنسان. مجلة جامعة دمشق للعلوم الاقتصادية والقانونية. مج ٢٧. العدد الأول. ص ص ٤٦١- ٤٨٧.

- عمر، أحمد مختار عبد الحميد. (٢٠٠٨). معجم اللغة العربية المعاصرة. الطبعة الأولى. دار عالم الكتب. مج ٣، ص ٢٤٦٢.
- قانون حماية البيانات الشخصية (قانون رقم ١٥١ لسنة 2020). جمهورية مصر العربية.
- نظام حماية البيانات الشخصية. (صادر بالمرسوم الملكي رقم (م/١٩) وتاريخ ٩/٢/١٤٤٣هـ). هيئة الخبراء بمجلس الوزراء. (https://laws.boe.gov.sa/boelaws/laws/lawdetails/b7cfae89-828e-4994-b167-adaa00e37188/1).

ثانيا: المراجع الأجنبية:

- Andreeva, K. & Kiseleva, A. (2021). Data Localization Laws: Russian Federation, Thomson Reuters Data Privacy Advisor. (https://www.morganlewis.com/-/media/files/publication/outside-publication/article/2021/data-localization-laws-russian-federation.pdf).
- Article 49 - Derogations for Specific Situations. Articles of the GDPR. Terms Feed. (https://www.termsfeed.com/blog/gdpr-articles/#Article_49_Derogations_For_Specific_Situations).
- Asymmetric Information. Corporate Finance Institute (CFI). (https://corporatefinanceinstitute.com/resources/wealth-management/asymmetric-information/).
- China: updates on international data transfers - security assessment requirements taking effect on 1 September. JDSUPRA. (https://www.jdsupra.com/legalnews/china-updates-on-international-data-3768008/)
- Data localisation may hit GDP, ease of doing business ranking, says report. Business Today. (https://www.businesstoday.in/latest/economy-politics/story/data-localisation-may-hit-gdp-ease-of-doing-business-ranking-says-a-report-111249-2018-11-20).
- Data Localization: An In-Depth Analysis. management study guide. (https://www.managementstudyguide.com/data-localization-an-in-depth-analysis.htm).
- Data privacy laws: What you need to know in 2023. OSANO. (https://www.osano.com/articles/data-privacy-laws#:~:text=U.S.%20data%20privacy%20laws,it%20still%20faces%20significant%20hurdles).
- Derogations for specific situations. GDPR. Art. 49. (https://gdpr-info.eu/art-49-gdpr/).
- Duggal, Pavan. (2019). Data localization: a review of proposed data localization legislation in India, with learnings for the United States. Data catalyst. (https://datacatalyst.org/wp-content/uploads/2020/06/data-localization-pavan-duggal.pdf)
- Elon Musk Completes $44 Billion Deal to Own Twitter. New York Times. (https://www.nytimes.com/2022/10/27/technology/elon-musk-twitter-deal-complete.html)
- Fraser, Erica. (2016). Data Localisation and the Balkanisation of the Internet. SCRIPTed. Volume 13, Issue 3. (https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/)
- General Data Protection Regulation. GDPR. (https://gdpr-info.eu/).
- Hong Y. (2019), Data Localisation: Deconstructing Myths and Suggesting a Workable Model for The Future. The Cases of China and The Eu. Working Paper. Brussels Privacy Hub.
- Largest tech companies by market cap. companies market cap. (https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/).
- National Security Letters. American Civil Liberties Union (ACLU). (https://www.aclu.org/other/national-security-letters).
- Population Data. The World Bank. (https://data.worldbank.org/indicator/SP.POP.TOTL).
- Russian Interference In 2016 U.S. Elections. FBI. (https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections).
- Shahbaz, Adrian. (2018). The Rise of Digital Authoritarianism. Freedom House. (https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism).
- Significance of data localisation for developing countries. iPleaders. (https://blog.ipleaders.in/significance-data-localisation-developing-countries/).
- Svantesson, D. (2020), "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", OECD Digital Economy Papers, No. 301, OECD Publishing, Paris.
- The 15 biggest data breaches of the 21st century. CSO online. (https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html).
- The Intelligence Collection Implications of the CLOUD Act. the Council on Foreign Relations (CFR). (https://www.cfr.org/blog/intelligence-collection-implications-cloud-act).

- The PRC Personal Information Protection Law (Final): A Full Translation. China Briefing. (https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/).
- The Real National Security Concerns over Data Localization. The Center for Strategic and International Studies (CSIS). (https://www.csis.org/analysis/real-national-security-concerns-over-data-localization).
- Transferring Personal Data Out of the EU. Terms Feed. (https://www.termsfeed.com/blog/transferring-data-out-eu/#Gdpr_Basics).
- Wei, Y. (2018), Chinese Data Localization Law: Comprehensive but Ambiguous. The Henry M. Jackson School of International Studies. University of Washington. (https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/).
- What is GDPR, the EU's new data protection law. GDPR. (https://gdpr.eu/what-is-gdpr/).

هوامش البحث

[1] انظر:
Hong Y. (2019), Data Localisation: Deconstructing Myths and Suggesting a Workable Model for The Future. The Cases of China and The Eu. Working Paper. Brussels Privacy Hub.

[2] المرجع السابق.

[3] عمر، أحمد مختار عبد الحميد. (٢٠٠٨). معجم اللغة العربية المعاصرة. الطبعة الأولى. دار عالم الكتب. ج ٣، ص ٢٤٦٢.

[4] المرجع نفسه، ج ١، ص ٢٧٥.

[5] منقول بتصرف عن:
Svantesson, D. (2020), "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", OECD Digital Economy Papers, No. 301, OECD Publishing, Paris.

[6] Hong Y. (2019).

[7] المرجع السابق.

[8] المرجع نفسه.

[9] ضوابط الأمن السيبراني للأنظمة الحساسة. الهيئة الوطنية للأمن السيبراني. المملكة العربية السعودية.)https://nca.gov.sa/legislation?item=177&slug=controls-list.(

[10] المرجع السابق.

[11] المرجع نفسه.

[12] Hong Y. (2019).

[13] GDPR. Art. 1. Subject-matter and objectives. (https://gdpr-info.eu/art-1-gdpr/).

[14] نظام حماية البيانات الشخصية. (صادر بالمرسوم الملكي رقم (م/١٩) وتاريخ ٩/٢/١٤٤٣هـ). هيئة الخبراء بمجلس الوزراء.)https://laws.boe.gov.sa/boelaws/laws/lawdetails/b7cfae89-828e-4994-b167-adaa00e37188/1.(

[15] The PRC Personal Information Protection Law (Final): A Full Translation. China Briefing. (https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/).

[16] Hong Y. (2019).

[17] عمران، ماجد؛ وكلثوم، فيصل. (٢٠١١). السيادة في ظل الحماية الدولية لحقوق الإنسان. مجلة جامعة دمشق للعلوم الاقتصادية والقانونية. مج ٢٧. العدد الأول. ص ص ٤٦١- ٤٨٧.

[18] المرجع السابق.

[19] المرجع نفسه.

[20] المرجع نفسه.

[21] المرجع نفسه.

[22] العتيبي، عبد الله بن جبر. (٢٠٠٩). العولمة وسيادة الدولة الوطنية: بحث في أهمية مفهوم السيادة في نظرية العلاقات الدولية. المجلة العربية للعلوم السياسية. عدد ٢٣. ص ص ٧١- ١١٢.

[23] Svantesson, D. (2020).

[24] Significance of data localisation for developing countries. iPleaders. (https://blog.ipleaders.in/significance-data-localisation-developing-countries/).

[25] The 15 biggest data breaches of the 21st century. CSO online. (https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html).

[26] المرجع السابق.

[27] Russian Interference In 2016 U.S. Elections. FBI. (https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections).

[28] Data Localization: An In-Depth Analysis. management study guide.

(https://www.managementstudyguide.com/data-localization-an-in-depth-analysis.htm).
[29] المرجع السابق.
[30] Largest tech companies by market cap. companies market cap.
(https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/).
[31] Elon Musk Completes $44 Billion Deal to Own Twitter. New York Times.
(https://www.nytimes.com/2022/10/27/technology/elon-musk-twitter-deal-complete.html)
[32] Data Localization: An In-Depth Analysis. management study guide.
(https://www.managementstudyguide.com/data-localization-an-in-depth-analysis.htm).
[33] المرجع السابق.
[34] Asymmetric Information. Corporate Finance Institute (CFI).
(https://corporatefinanceinstitute.com/resources/wealth-management/asymmetric-information/).
[35] Data Localization: An In-Depth Analysis. management study guide.
(https://www.managementstudyguide.com/data-localization-an-in-depth-analysis.htm).
[36] Duggal, Pavan. (2019). Data localization: a review of proposed data localization legislation in India, with learnings for the United States. Data catalyst.
(https://datacatalyst.org/wp-content/uploads/2020/06/data-localization-pavan-duggal.pdf)
[37] Data localisation may hit GDP, ease of doing business ranking, says report. Business Today.
(https://www.businesstoday.in/latest/economy-politics/story/data-localisation-may-hit-gdp-ease-of-doing-business-ranking-says-a-report-111249-2018-11-20).
[38] Duggal, Pavan. (2019).
[39] Data Localization: An In-Depth Analysis. management study guide.
(https://www.managementstudyguide.com/data-localization-an-in-depth-analysis.htm).
[40] Shahbaz, Adrian. (2018). The Rise of Digital Authoritarianism. Freedom House.

(https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism).

[41] Fraser, Erica. (2016). Data Localisation and the Balkanisation of the Internet. SCRIPTed. Volume 13, Issue 3.
(https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/)
[42] National Security Letters. American Civil Liberties Union (ACLU).
(https://www.aclu.org/other/national-security-letters).
[43] المرجع السابق.
[44] Andreeva, K. & Kiseleva, A. (2021). Data Localization Laws: Russian Federation, Thomson Reuters Data Privacy Advisor.
(https://www.morganlewis.com/-/media/files/publication/outside-publication/article/2021/data-localization-laws-russian-federation.pdf).
[45] China: updates on international data transfers - security assessment requirements taking effect on 1 September. JDSUPRA. (https://www.jdsupra.com/legalnews/china-updates-on-international-data-3768008/)
[46] المرجع السابق.
[47] Wei, Y. (2018), Chinese Data Localization Law: Comprehensive but Ambiguous. The Henry M. Jackson School of International Studies. University of Washington.
(https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/).
[48] What is GDPR, the EU's new data protection law. GDPR.
(https://gdpr.eu/what-is-gdpr/).
[49] General Data Protection Regulation. GDPR.
(https://gdpr-info.eu/).
[50] انظر:
Transferring Personal Data Out of the EU. Terms Feed.
(https://www.termsfeed.com/blog/transferring-data-out-eu/#Gdpr_Basics).
[51] Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection. European Commission.
(https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#:~:text=The%20European%20Commission%20has%20so,Uruguay%20as%20providing%20adequate%20protection).

[52] Derogations for specific situations. GDPR. Art. 49.
(https://gdpr-info.eu/art-49-gdpr/).
[53] Article 49 - Derogations for Specific Situations. Articles of the GDPR. Terms Feed.
(https://www.termsfeed.com/blog/gdpr-articles/#Article_49_Derogations_For_Specific_Situations).
[54] Data privacy laws: What you need to know in 2023. OSANO.
(https://www.osano.com/articles/data-privacy-laws#:~:text=U.S.%20data%20privacy%20laws,it%20still%20faces%20significant%20hurdles).
[55] The Real National Security Concerns over Data Localization. The Center for Strategic and International Studies (CSIS).
(https://www.csis.org/analysis/real-national-security-concerns-over-data-localization).
[56] المرجع السابق.
[57] The Intelligence Collection Implications of the CLOUD Act. the Council on Foreign Relations (CFR).
(https://www.cfr.org/blog/intelligence-collection-implications-cloud-act).
[58] المرجع السابق.
[59] المرجع نفسه.
[60] Population Data. The World Bank.
(https://data.worldbank.org/indicator/SP.POP.TOTL).
[61] قانون حماية البيانات الشخصية (قانون رقم ١٥١ لسنة ٢٠٢٠). جمهورية مصر العربية.
[62] المرجع السابق.
[63] نظام حماية البيانات الشخصية. (صادر بالمرسوم الملكي رقم (م/١٩) وتاريخ ٩/٢/١٤٤٣هـ). هيئة الخبراء بمجلس الوزراء.
) https://laws.boe.gov.sa/boelaws/laws/lawdetails/b7cfae89-828e-4994-b167-adaa00e37188/1.(
[64] "سدايا" تعلن تأجيل العمل بنظام حماية البيانات الشخصية. وكالة الأنباء السعودية.
)https://www.spa.gov.sa/2339723.(