اتجاه الدول نحو تبني سياسات توطين البيانات:
دراسة في: المفهوم، الدوافع، والاشتراطات، والمتطلبات
The trend of countries towards adopting data localization policies,
'A study in concept, motives, conditions, and requirements'

دينا فتحي جمعة عبدالعظيم

طالب ماجستير – كلية السياسة والاقتصاد – جامعة بني سويف

عبدالرحمن عبدالعال خليفة

أستاذ العلوم السياسية المساعد بكلية السياسة والاقتصاد – جامعة بني سويف

رضوي سيد أحمد محمود

مدرس العلوم السياسية بكلية السياسة والاقتصاد – جامعة بني سويف

المستخلص:

تمثل البيانات أحد أهم الموارد الحيوية في عصر المعلومات الحالي، كونها ترتبط بكافة التعاملات والتداولات الرقمية التي تتم من خلال شبكة الإنترنت، وذلك من خلال تدفقها الحر عبر الحدود الوطنية للدولة، وهو ما يضمن استمرار كافة النشاطات المرتبطة بها، سواء كانت اجتماعية، اقتصادية، تجارية، سياسية، معلوماتية، أمنية وحتى عسكرية، ولما كان هذا التدفق الحر في حد ذاته – الذي يضمن إتاحة البيانات الشخصية وغير الشخصية على نطاق واسع في ظل واقع افتراضي يتمتع بقدر كبير من الحرية دون قيود ملموسة تحدد نطاق تعاملاته ونشاطاته– عُرضة للتهديدات والمخاطر وذلك كونه ينتقل للتخزين في خوادم أجنبية عبر شبكات رقمية غير مؤمنة على النحو الأمثل ولا تخضع لرقابة وسيطرة الدولة الوطنية، مما يجعلها عُرضه لانتهاك الخصوصية من جانب، واستغلالها لصالح الجهات الحاضنة لها من جانب آخر، وهو ما قد ينعكس بدوره سلبًا على الأمن القومي للدولة المالكة لها، وهو ما يؤدي بالدول لاتباع سياسات توطين البيانات لتحقيق عدة دوافع، وفق عدد من الاشتراطات والمتطلبات التي تتراوح ما بين إنفاذ القانون المحلي، والحد من التدخل الأجنبي في شئون الدولة، وحماية الخصوصية، وتعزيز السيادة الوطنية من خلال تنمية مفهوم السيادة الرقمية، وأخيرًا تعزيز الاقتصاد القومي المحلي.

الكلمات المفتاحية؛ توطين البيانات، أمن البيانات، حماية الخصوصية، إنفاذ القانون، سيادة البيانات.

Abstract:

Data represents one of the most vital resources in the current information age, as it is linked to all digital transactions and trades that take place through the Internet, through its free flow across the national borders of the state, which ensures the continuation of all activities associated with it, whether social,

economic, commercial, political, informational, security and even military, and since this free flow in itself - which ensures the availability of personal and non-personal data on a large scale in light of a virtual reality that enjoys a great deal of Freedom without tangible restrictions that determine the scope of its transactions and activities - vulnerable to threats and risks as it moves to storage in foreign servers through digital networks that are not optimally secured and are not subject to the control and control of the national state, which makes it vulnerable to violation of privacy on the one hand, and its exploitation for the benefit of its incubators on the other hand, according to a number of requirements and requirements These range from enforcing domestic law, limiting foreign interference in state affairs, protecting privacy, strengthening national sovereignty through the development of the concept of digital sovereignty, and finally strengthening the local national economy.
Keywords: data localization, data security, privacy protection, law enforcement, data sovereignty.

المقدمة:

تمثل البيانات أحد أهم الموارد الحيوية في عصر المعلومات الحالي، كونها ترتبط بكافة التعاملات والتداولات الرقمية التي تتم من خلال شبكة الإنترنت، وذلك من خلال تدفقها الحر عبر الحدود الوطنية للدولة، وهو ما يضمن استمرار كافة النشاطات المرتبطة بها، سواء كانت اجتماعية، اقتصادية، تجارية، سياسية، معلوماتية، أمنية وحتى عسكرية إن تطلب الأمر، ولما كان هذا التدفق الحر في حد ذاته – الذي يضمن إتاحة البيانات الشخصية وغير الشخصية على نطاق واسع في ظل واقع افتراضي يتمتع بقدر كبير من الحرية دون قيود ملموسة تحدد نطاق تعاملاته ونشاطاته– عُرضة للتهديدات والمخاطر وذلك كونه ينتقل للتخزين في خوادم أجنبية عبر شبكات رقمية غير مؤمنة على النحو الأمثل ولا تخضع لرقابة وسيطرة الدولة الوطنية، مما يجعلها عُرضه لانتهاك الخصوصية من جانب، واستغلالها لصالح الجهات الحاضنة لها من جانب آخر، وهو ما قد ينعكس بدوره سلبًا على الأمن القومي للدولة المالكة لها، لذا قد اتجهت العديد من الدول لتبني حِزمة من الإجراءات والتدابير لحماية السيادة الوطنية لها بمفهومها المعاصر، من خلال تنظيم عملية انتقال تلك البيانات عبر حدود الدولة وذلك بانتهاج سياسات يطلق عليها "**توطين البيانات**"، والتي تستهدف خِلالها تخزين البيانات داخل حدود الدولة لمنع انتقالها ومعالجتها في الخارج، وذلك في ظل دوافع عِدة تندرج تحت مظلة حماية الأمن القومي، وأمن المعلومات ولاسيما المعلومات الاستراتيجية الهامة.

ولما كانت البيانات بمثابة هاجس أمني للعديد من الدول، فجاءت الإجراءات والتدابير التي اعتمدتها تلك الدول بشأن حمايتها من خلال اتباع سياسات توطين البيانات، سواء كان من خلال التشريعات القانونية أو الإجراءات التقييدية لعملية انتقال البيانات عبر الحدود الوطنية، ولكن بالبحث العميق في هذا الأمر

يتضح أن تلك الدول محكومة بالعديد من الدوافع الصريحة منها والضمنية، وذلك لتحقيق عدة أهداف سياسية، اقتصادية، أمنية، واجتماعية، لذا سيتم تقسيم الدراسة وفقًا لهذا الأمر.

أولاً – الإشكالية البحثية الدراسة

تدور إشكالية الدراسة حول الجدل بشأن تأثير توطين البيانات على الأمن القومي للدول، والذي يعد بمثابة هاجس للعديد من الدول كونه يرتبط بالمعلومات والبيانات الحيوية التي تمس أمن الفرد والدولة على حد سواء – فمن جانب هناك بعض الدول تدعم السياسات المفتوحة في إتاحة البيانات لمواطنيها إذ ترى أنه حق أصيل للمواطن وتسمح كذلك بالتدفق الحر لها عبر الحدود لمعايير المعالجة والتخزين، وعلى الجانب الآخر هناك دول أخرى تسعى لتقييد تدفق بياناتها عبر الحدود بداعي حماية خصوصية مواطنيها، وتتحفظ على إتاحة بعضها داخليًا وذلك لحماية أمن المعلومات الخاصة بها – وبما أن الدول تتفاوت من ناحية البنى التحتية التكنولوجية وهو ما يصنفها لدول تصنع التكنولوجيا ودول مستوردة لها، ودول متقدمة في تلك الصناعة وأخرى نامية، لذا فإنه عند التطرق لمسألة توطين البيانات فإن هنالك إشكالية ترتبط بمدى تأثر تلك الدول وفقًا لمقدراتها وإمكاناتها بتلك السياسات، ومقدار النفع والضرر الواقع عليها، ومدى استجابتها في التفاعل مع تلك الظرفيات.

- **<u>التساؤل الرئيس للدراسة؛</u>**

في نطاق محاولة رصد النطاق الذي تؤثر من خلاله تلك السياسات على الأمن القومي للدولة وذلك وفقًا لإمكاناتها وقدراتها، يمكن طرح التساؤل كما والتالي؛ " **إلى أي مدى تؤثر سياسات توطين البيانات على الأمن القومي للدول؟**"، ويتفرع منه عدد من المفاهيم الفرعية؛

- ماهية توطين البيانات؟
- ماهي دوافع الدول لتطبيق سياسات توطين البيانات؟
- ما هي الاشتراطات والمتطلبات المتبعة لتبني سياسات توطين البيانات؟

ثانيًا – المنهج المستخدم:

يستخدم الباحث بمنهجيتين، **الأولى** تتمثل في **نظرية النظم** وفقًا لتحليل "كارل دويتش"، حيث يعتمد على ما يتدفق للنظام من بيانات ومعلومات من البيئة الداخلية والخارجية ويتم جمعها لرصد تأثيرها على عملية صنع القرار فيما يتعلق باتباع سياسات توطين البيانات، و**الثاني**؛ اقتراب "**الحوكمة**" ليعبر عن إجمالي القرارات والتشريعات التي تتخذها الحكومة لأجل تدعيم تلك السياسات، وحيثياته وظروف اتخاذه.

ثالثًا – تقسيم الدراسة:

- **المحور الأول؛ مفهوم توطين البيانات.**
- **المحور الثاني؛ دوافع الدول لتبني سياسات توطين البيانات.**

- **المحور الثالث؛ الاشتراطات والمتطلبات لتبني سياسات توطين البيانات.**

المحور الأول: مفهوم توطين البيانات

البيانات عبارة عن عملية تحمل نصوص أو رموز أو مفاهيم صماء تخضع للمعالجة من قِبل الإنسان أو أجهزة الحاسب الآلي من أجل فك شيفراتها لتضحى بمثابة معلومات قَيْمة تخدم الغرض منها أو المجال الذي تستهدفه، وبدمج التوطين والبيانات بمدلوليهما، فيشير المصطلح إلى عملية تخزين وتجميع النصوص أو البيانات، والمعلومات التي تخص دولة ما أو مواطنيها داخل حدودها، وأن يتم معالجتها داخل النطاق الوطني للدولة، وأشارت العديد من الدراسات إلى تعريفات متباينة لفظيًا لمصطلح توطين البيانات، ولكنها تحمل ذات المدلول السالف الإشارة إليه، ولعل من أبرز التعريفات ما يلي؛

أولًا، تم ربط المصطلح بالمراكز المختصة الوطنية في مجال الحوسبة السحابية وخدمات الفضاء الإلكتروني، ولكن في نطاق حدود الدولة، لذا عُرف بأنه "العملية التي يصاحبها التخزين لبيانات المستخدم في مراكز مختصة لجمع البيانات على شبكة الإنترنت وذلك داخل حدود الدولة التي تخصها تلك البيانات".[١]

ثانيًا؛ ممارسة تخزين البيانات على أي جهاز حاسب آلي داخل حدود الدولة، من خلال خوادم تخضع لسيطرة الدولة، ففي تلك العملية يتم إخطار الشركات التي تعمل في مجال الحوسبة السحابية أن تقوم بتخزين البيانات الخاصة بمواطنيها داخل حدود دولتها دون تخزينها في مقر الدولة التي تنتمي لها تلك الشركات الأجنبية، أي أنها عملية القيد على التدفق الحر للبيانات عبر الحدود،[٢] والجدير بالذكر أنه في هذا قد ركز على الخوادم الوطنية التي تخضع لسيادة الدولة، ليتم ممارسة عملية التوطين للبيانات داخلها، ولم يتطرق للخوادم الدولية أو العالمية التي تخص الشركات الأجنبية مقدمة الخدمة الإلكترونية.

ثالثًا؛ في موضع آخر تمت الإشارة لمفهوم التوطين للبيانات باعتباره، ممارسة الحد الأدنى من تخزين البيانات والمعلومات داخل حدود الدولة، أو حتى الالتجاء إلى نقل البيانات في مناطق جغرافية محددة، [٣] تطرق التعريف لمنطوق الحد الأدنى، ليشير أنه قد لا يتم الممانعة في انتقال البيانات الشخصية عبر الحدود الوطنية إذا ما كانت تخدم مصلحة الفرد، ولكن بالامتثال لمعايير الخصوصية فإن ممارسة الحد الأدنى تعني تخزين البيانات ومعالجتها داخل نطاق الدولة، وتخضع لمعايير أمان الدولة السيبراني ثم يتم السماح لها بالانتقال.

رابعًا؛ تعبر عن كافة الإجراءات والتدابير التي يتم اتخاذها من قِبل دولة ما لحماية البيانات الشخصية لمواطنيها من أن يتم نقلها وتخزينها ومعالجتها خارج الحدود الوطنية لها من خلال دولة المنشأ

للشركات المُكلفة، وعادة ما تشمل تلك الإجراءات تقنين القواعد والقوانين القائمة في مجال حماية البيانات وحماية الخصوصية وليس من خلال إنشاء قوانين وقواعد جديدة مغايرة لتلك المتواجدة. (٤)

وأخيرًا، هنالك تعريف لتوطين البيانات باعتبارها أنها كافة السياسات والآليات والبرامج التي يتم من خلالها إدارة البيانات المرتبطة بالأفراد سواء كانت شخصية أو صحية أو مالية أو تجارية، أو تلك البيانات المرتبطة بهيكل ومؤسسات الدولة، بحيث يتم الامتثال لتلك التفويضات وأن تُخزن داخل النطاق الجغرافي الخاص بالدولة ذات الصلة بتلك البيانات، وهو بالأمر الذي قد يستدعي التفرقة بين البيانات الشخصية، والبيانات الشخصية الحساسة والبيانات الشخصية الهامة،(٥) يعد هذا المفهوم أحد أبرز التعريفات الشاملة لمصطلح توطين البيانات، كونه تطرق إلى جوهر المفهوم، والجزء الفني الذي من خلاله سيتم الانتقال للتطبيق الفعلي لعمليات التوطين، بمعنى أنه أشار إلى مجمل السياسات والإجراءات الفنية التي تتخذها من طلبات تنقيح للقوانين المحلية والدولية أو اقتراح بنود تعديلية على التشريعات المرتبطة بتنظيم التدفق الحر للبيانات عبر الحدود الوطنية للدولة، وتلك المختصة بحماية الخصوصية.

المحور الثاني؛ دوافع الدول لتبني سياسات توطين البيانات

عقب تسريبات "سنودن"، سارعت الدول للتحرك فرادى كانت أم جماعيًا لأجل حماية البيانات والمعلومات التي تتدفق خارج حدودها سواء كانت الشخصية أو البيانات الحساسة ذات الأهمية الاستراتيجية للدولة، والتي تم اكتشاف أنها مورد خصب للاستخدام غير القانوني وغير العادل، بالإضافة للاختراقات السيبرانية، وكانت تحركات تلك الدول في بادئ الأمر بدافع حماية الأمن القومي لها، بمفهومه الفضفاض غير المحدد، ولكن سرعان ما جزئت الدول أهدافها من تبني تلك السياسات، وذلك لتصب في صالح الدولة وأهدافها التي تسعى لتحقيقها، لذا إذا كان هنالك من داعٍ لتقسيم تلك الدوافع، فإنها لن تخرج عن تلك العناصر، **الدوافع السياسية**؛ لتشمل السيادة الوطنية للدولة على البيانات، إنفاذ القانون المحلي والامتثال القضائي، الحد من الوصول الأجنبي للبيانات، ضمان سيطرة الدولة على منافذ البيانات "الرقابة"، الحد من المخاطر الجيوسياسية ومكافحة الفكر الرأسمالي القائم على تبني مبادئ العولمة، وأخيرًا تعزيز روابط المجتمع، وعن **الدوافع الأمنية**؛ حماية الأمن السيبراني لتعزيز الأمن القومي، والرقابة على المعلومات، في حين تأتي **الدوافع الاقتصادية**؛ ممثلة في تشجيع الاقتصاد المحلي في مواجهة الشركات العابرة للقوميات ومحتكرة صناعة التكنولوجيا، **الدوافع التكنولوجية**؛ بناء شبكات معلوماتية محلية مستقلة، تعزيز البنى التحتية التكنولوجية، وفيما يأتي توضيحها؛

أولًا الدوافع السياسية؛

جاءت أهداف الدولة السياسية فيما يتعلق بتبني سياسات توطين البيانات؛ في تعزيز السيادة الوطنية، إنفاذ القانون المحلي وحماية الأمن القومي، حماية الخصوصية للمواطنين، سيطرة الحكومة على

البيانات المخزنة خارجيًا، الحد من الوصول الأجنبي للبيانات، الحد من المخاطر الجيوسياسية، مواجهة متطلبات العولمة وتتمثل في؛

١. تعزيز السيادة الوطنية "السيادة الرقمية للبيانات"؛

تأتي مساعٍ الدول فيما يتعلق بتوطين البيانات، وذلك لأجل تعزيز مفهوم السيادة الوطنية بصورتها المعاصرة المرتبطة بالبيانات أو ما يمكن أن يطلق عليه تحقيق "السيادة الرقمية"، فالسيادة تتنافى مع التدفق الحر للبيانات في الفضاء السيبراني، لذا تهدف الدولة لتحقيق الاستقلالية عن الشبكة العنكبوتية، وإنشاء نظام محلي موازٍ للنظام الرقمي المفتوح، لتضمن سيطرتها على تدفقات البيانات، وتحد من الاستخدامات غير القانونية لها، وذلك تحت مزاعم إعادة مفهوم القومية، [٦] وعلى اعتبار أن الفضاء السيبراني أتاح العلمانية بمعنى الانفتاح المعلوماتي وذلك لاعتماده تدفق البيانات وانتقالها للخارج للمعالجة، ففكرة الحدود في ظل الثورة المعلوماتية أضحت غير ذات الأهمية، وهذا ما يتنافى مع مفهوم الدولة القومية التي تحكم قبضتها على الشأن الداخلي، وتحكمها حدود داخلية وخارجية، ولكنها من جانب آخر تفقد السيطرة على تلك البيانات التي تعتبرها جزء يخص أمن الدولة القومي، وانتقاله دون اتباع معايير الحماية والخصوصية يعرض الدولة للمخاطر، ويُفَرغ مفهوم السيادة الوطنية من مضمونه، لذا فالهدف الجلي لصانعي السياسات هو السيطرة التامة والتحكم في البيانات، وتخزينها داخليًا من خلال متطلبات صارمة على مزودي خدمات الإنترنت، والحد من انتقالها للدول الأجنبية للمعالجة والتخزين، وكان أبرز **مثال لتطبيق سياسات التوطين للبحث عن السيادة المفقودة**، كل من **ألمانيا، وفرنسا**، الدولتين الأوربيتين، الأكثر تضررًا من الاستخدام غير المشروع للبيانات في أعمال الرقابة والتجسس من قبل الجانب الأمريكي، فقد دعت المستشارة الألمانية "ميركل"، والرئيس الفرنسي" ماكرون" لاتباع سياسات أكثر صرامة لأجل تحقيق السيادة الرقمية على البيانات، لأن تخزين البيانات الأوروبية على خدمات الحوسبة السحابية لدولة أجنبية يجعل الدولة منقوصة السيادة، ومعرضة للرقابة المستمرة والضغط الأجنبي، ومنه لتهديد الأمن القومي والمعلوماتي للدول كما وحصل سابقًا، لذا سعت نحو الحفاظ على الهوية الأوروبية وذلك من خلال اشتراطات التخزين المحلي، للتخلص من الاستعمار الرقمي الأجنبي لبيناتهم، وباعتبار أن تلك الدولتين تمتلكان قواعد بيانات حساسة وبالأخص أنها دول صناعية بالدرجة الأولى. [٧]

٢. إنفاذ القانون المحلي "الامتثال القضائي"؛

بررت العديد من الدول اتباعها سياسات توطين البيانات، لمساعدة الجهات القانونية والقضائية للوصول للبيانات، وبخاصة في القضايا التي تتطلب البيانات والمعلومات الرقمية، كغسيل الأموال، مكافحة الفساد، وحتى قضايا مكافحة الإرهاب داخليًا، والجرائم الجنائية، فتوطين البيانات يجعل الوصول للمعلومات من قِبل الجهات القضائية أيسر من ذي قبل وفق ما تعتقد، حيث سابقًا كان يتعين على الدولة أن تتقدم

بطلب إلى الجهات الأجنبية التي تُخَتَزن فيها تلك المعلومات، وبالتالي كان يقابل إما بالرفض لإجراءات الخصوصية أو القبول ولكن يصحبه طول الفترة الزمنية للإفراج عنها، فكان الوصول للبيانات مقيدًا بتدابير صارمة،[٨] ولكن مع تواجد خوادم وطنية داخل حدود الدولة لتخزين البيانات الشخصية وغير الشخصية الهامة، يُسهل من عمل الجهات القضائية والقانونية فيما يتعلق بجمع أدلة الإثبات أو الإدانة ولاسيما إذا كانت المعلومات الرقمية ضمن دائرة اختصاصها في القضية المطروحة، فتعتقد الدول أن الوصول غير المقيد للبيانات هو أمر سيساعد جهات إنفاذ القانون للقيام بعملها بشكل سلس، كما أن التخزين المحلي للبيانات سيحد من التدخل الأجنبي فيما يتعلق بالاطلاع على الغرض من الحصول على البيانات، والتي تعد بمثابة أمر سري يخص الجهة القضائية للدولة صاحبة البيانات، فالحكومات تظن أن التوطين سيمنع الوصول الأجنبي للبيانات، وبالتالي لن تتوقف عمليات التحقيق.[٩]

ولكن بالنظر إلى ما تعنيه مفاهيم توطين البيانات، ففكرة نقل تخزين البيانات من خارج حدود الدولة إلى داخل حدودها، فهو إن كان سيغير مكان التخزين لكنه لن يغير الجهة المسئولة عن التخزين والمعالجة المحلية، بمعنى أن مزودي أو مقدمي خدمات الإنترنت للدولة المستهدفة التخزين الداخلي، لن تسمح للدولة بأن تمتلك خوادم التخزين لأنها ستبنى خوادمها الخاصة بالتخزين في الدولة المالكة للبيانات، وإذا امتلكتها لن تكون جهة الرقابة على تلك البيانات، ومنه ستضطر الدولة كذلك لاتباع ذات الإجراءات والتدابير لطلب الوصول للبيانات الخاصة بجهات إنفاذ القانون هذا من جانب، أما الجانب الآخر محل الجدل في تلك المسألة؛ إذا كانت الدول تسعى للوصول الآمن غير المقيد للبيانات، فإجراءات التوطين ليست الخيار الأمثل لهذا الأمر، إذ أن هنالك معاهدات ثنائية وجماعية بين الدول وبعضها بعضًا لضمان الوصول غير المقيد للبيانات وذلك لضمان تحقيق العدالة القانونية، **كأمثال قانون 'cloud' الأمريكي**،[١٠] الذي يتيح للدول الحصول على المعلومات الخاصة بها إذا ما كانت طرفًا في معاهدة ثنائية مع الولايات المتحدة الأمريكية، وبالتالي دافع التوطين لأجل إنفاذ القانون غير مدعم بالحُجج المقنعة من قِبل الدول أو أنه قد يكون مظلة علنية لأخرى ضمنية مرتبط بسعي الدولة للسيطرة على بيانات مواطنيها ومراقبتها تحت مظلة إنفاذ القانون.

فعلى سبيل المثال؛ استعانت الهند بتكنولوجيا المعلومات لاستخدامها في إنفاذ القانون الجنائي من خلال كاميرات المراقبة ذات الدوائر المُغلقة، لمراقبة الشوارع والأماكن العامة، ورصد أي أفعال غير قانونية مُشتبه بها في أية جُرم جنائي، بالفعل وجهت بإنشاء مركز رقابة مركزية، يتضمن كافة البيانات والمعلومات الجغرافية والشخصية بداخله، ليستخدمها لأجل حل الجرائم الجنائية المُعقدة، وهي مفترض أنها تطلب إتاحة كافة المعلومات عن المواطنين، بالإضافة للمعلومات الجغرافية عن موقعهم وتفاصيل عناوينهم، ليتم الرصد والتتبع من جانب هذا المركز، ويُذكر أن نظام مراقبة كاميرات الدوائر المُغلقة يتم استخدامه في أكثر من

١٥ مدينة هندية بواقع ١.٥٤ مليون كاميرا، وأن ما يقرب من ٩١٪ من إجمالها في كل من مدينة "نيودلهي"، "وحيدر آباد"، "وتشيناي"، "وإندور". وبالرغم من اعتماد تلك المنهجية لمساعدة إنفاذ القانون المحلي جنائيًا، إلا أنه لم يغفل الزيادة في أعداد الجرائم الجنائية داخل الهند لتصل لنحو ٣٢٠٠٠ جريمة خلال عام ٢٠١٨، كما أنه أثار قلق المواطنين كون تُعرض خصوصيتهم للانتهاك، وشعورهم بعدم الراحة بأنهم مراقبين في كافة الأنحاء من جانب، وبياناتهم الشخصية ومواقعهم الجغرافية متاحة للوصول من جانب مركز المراقبة المركزي الهندي.(١١)

٣. الحد من الوصول الأجنبي للبيانات "منع التدخل في شئون الدولة"؛

يعد هذا البند أحد أهم الدوافع المرتبطة بسياسات توطين البيانات، حيث أن نقل البيانات للخارج للمعالجة والتخزين هو أحد المؤرقات التي تصيب صانع القرار السياسي داخليًا، وذلك لأن تلك البيانات عُرضة للمراقبة الأجنبية من قبل الدول المستقبلة لها، وتمثل الموطن الأم للشركات الحاضنة لتلك البيانات، وهو ما تم إثباته فعليًا بتسريبات سنودن في صحيفة الجارديان، وبالأخص النفوذ الواسع لوكالة الأمن القومي الأمريكية وقدرتها على التوغل داخل الدول من خلال ترصد الألياف الضوئية لأسلاك الإنترنت، لجمع المعلومات والبيانات الخاصة بشعوب وحكومات الدول، فعلى سبيل المثال جاءت الخريطة الحرارية للهند ضمن النطاق الواقع بين اللون البرتقالي الذي يميل نحو الأحمر، أي أنها تمثل نقطة ارتكاز محورية للمراقبة من الجانب الأمريكي، وجدير بالملاحظة أن تلك الوثائق أشارت كذلك أنه في مارس ٢٠١٣ قد تم استهداف نحو ٦.٣ مليار نسخة إلكترونية لبيانات هندية مرتبطة بشبكة الإنترنت للمستخدمين الهنود، بالإضافة إلى ٦.٢ مليار نسخة إلكترونية للبيانات المرتبطة بسجلات المكالمات الهاتفية. (١٢) لذا عمدت الدول للحد من نقل البيانات للخارج وتخزينها داخل خوادم مركزية تخضع لسلطة الدولة، (١٣) فجاء هذا الدافع ضمانة لعدم التدخل الخارجي في شئون الدولة، بمعنى أن الدول من الممكن باطلاعها على البيانات الخاصة بمواطنيها سواء كانت شخصية أو حساسة للغاية، فإنها بذلك قد توغلت داخل النسيج المجتمعي للدولة، وبالأخص إذا كانت دولة تتسم بالتنوع العرقي والإثني والاختلاف الطائفي.

لذا قد تستغل تلك النقاط لاستغلال السلطة السياسية إما بتغيير موقف تجاه قضية معينة أو اتخاذ قرار يخدم مصالح تلك الدولة أو إذا ما كان هذا النظام يعارض توجهاتها، فإنها قد تنزع فتيل التقسيم العرقي من خلال بث الطائفية والشقاق بين أفراد المجتمع واستغلاله ضد الدولة بهدف زعزعة الاستقرار والأمن ومنه لتنحي النظام السياسي، ففكرة الوصول الأجنبي للبيانات التي تخص دولة بعينها، فهذا دليل على عنصر الاختراق الأمني والتهديد المباشر للأمن القومي للدولة، هذا على صعيد البيانات الشخصية، أما إذا ما كانت هنالك بيانات اقتصادية وتجارية يتم نقلها للخارج بغرض التخزين والمعالجة وتخص الأنظمة المالية والاقتصادية، فالوصول الأجنبي لها، دليل على أن الدولة أصبحت مباحة في كافة سياساتها،

وأهدافها، وقد تكون عُرضة للهجوم المباشر وقد يتم توجيهه لقطاع المال والأعمال، ضرب العملة أو النظام الأمني من خلال الإرهاب الإلكتروني أو التجسس على الجهات الحكومية وكبار المسئولين، لذا فهذا الدافع الأكثر منطقية ومشروعية ويتسق مع حق الدولة في عدم التدخل في شئونها الداخلية من قبل الغير، وفق ما تنص عليه المواثيق الدولية وعلى الميثاق العام للأمم المتحدة، وبالتالي باتباع الدولة لتدابير توطين البيانات فهذا سيحجب البيانات الحساسة عن الوكالات الاستخباراتية، بمعنى أن التخزين داخل الولايات المتحدة أو أية دولة على غرارها لأغلب مقدمي خدمات الإنترنت كان يسهل من الوصول للبيانات وتنفيذ المراقبة العامة على قواعد البيانات سواء بجانب غير قانوني أو قانونيًا لأغراض الأمن القومي، ولكن بقيام الدول تباعًا بطلب التخزين المحلي ومنع انتقالها للخارج فهو لن يحمي البيانات كليًا من الوصول الأجنبي لها، ولكنه سيزيد من تعقيد عملية الوصول لأنها ستزيد من التكلفة المالية للقيام بتلك العملية في دول عدة.(١٤)

٤. الحد من التهديدات الجيوسياسية؛

تمثل خدمات الموقع الجغرافي أحد أهم مزايا الثورة الصناعية الرابعة، وذلك لأنها ساهمت بتذليل الصعوبات المرتبطة بالموقع، وبالأخص للأفراد في حال ارتادوا أي دولة بغرض السياحة أو العمل أو الدراسة، وخدمات الموقع تتطلب تخزين البيانات والمعلومات المرتبطة بالمكان، وتفاصيل تخصه، سواء كان الخدمات التي يقدمها، الموقع التفصيلي له، والمزايا التي يتضمنها، وكافة البيانات التي تفيد الشخص الأجنبي مرتاد الدولة، ويتم تحديد المكان وفق الاتصال بالأقمار الصناعية وإمدادها بتلك المعلومات ومنه لتحديد الموقع المراد الوصول له، كما يتم وفقًا شركة 'google earth'، ولكن بالتدقيق في هذا الأمر يتضح أن خدمات الموقع الجغرافي وغيرها من الخدمات الأخرى ذات الصلة، قد تشكل تهديدًا للأمن القومي للدول المستهدفة، حيث أنها قد تستفيد بمعلومات وبيانات تخص مواقع استراتيجية.

بالإضافة لتوجيه تلك الأقمار الصناعية لأغراض تصوير المواقع اللوجستية للدولة أو توجيه ضربات استباقية كما وطائرات "Drone"، لصالح وكالات الاستخبارات الأجنبية، أو أن يتم الوصول غير القانوني لتلك البيانات لها وفق البرمجيات الضارة الخبيثة التي تتبعها الوكالات الأمنية، كبرامج الاختراق الخبيثة التي تمتلكها المخابرات الأمريكية وتحصل من خلالها على البيانات، فقد كشفت التسريبات أن **الهند** كان يتم الحصول على بياناتها من خلال برنامجين، **الأول**؛ **'Boundless Informant'**، عبارة عن برنامج للبحث والتتبع للبيانات من خلال رصد رسائل البريد الإلكتروني والمكالمات الهاتفية، وبالتالي تعرضت البيانات الهندية المستهدفة إلى هذا البرنامج للتعرف والتنقيب عن البيانات المهمة بها، والتي تخص الأمن القومي الهندي، سواء كانت بيانات شخصية وحكومية أو تجارية، **الثاني**؛ برنامج **"PRISM"**، والمختص بتعقب المحتوى الذي يُقدم عبر شبكة الإنترنت، واستخدمته وكالة الأمن القومي الأمريكية لأجل

جمع البيانات حول العديد من الملفات الحرجة، من خلال بيانات الخدمات المرتبطة بشبكة الإنترنت، كأمثلة؛ "Google"، "Microsoft" ، "Facebook"، "Yahoo"، "Apple"، "YouTube" لذلك اعتبرت الدولة أن اتباع منهجيات توطين البيانات، إنما هو بهدف دفع تلك التهديدات عن الدولة، حيث أنه ستطلب من مزودي تلك الخدمات بأن يتم تخزين البيانات داخل حدود الدولة وفق الخوادم المركزية، ومنع انتقالها للخارج لأجل ضمان سريتها وعدم الاضطلاع عليها، بالإضافة أن هنالك العديد من الدول التي فرضت اشتراطات على التخزين لتلك البيانات وذلك لاعتبارها معلومات سرية للغاية وتمثل تهديد صريح ومباشر للأمن القومي للدولة، وتستهدف السيادة لها على نحو مباشر إذا ما تم تتبع الموقع وفق برمجيات متقدمة تابعة لأنظمة بعينها، وعلى اعتبار أن هذا البند يعد من صميم الملفات الجيوسياسية، فإنه بذات الأهمية لتعتبره الدولة ضمن الدوافع الجوهرية لتبني سياسات توطين البيانات. (١٥)

كما أنه من المخاطر الجيوسياسية الأخرى المحتملة، فكرة تدفق البيانات وانتقالها خارج حدود الدولة، من خلال الكابلات المتواجدة تحت سطح البحر، وبالتالي فإن تواجد تلك الكابلات تحت عمق الماء، إنما هو يعني سهولة الوصول لها من قِبل مخترقي النظام الشبكي، وهو ما قد يتسبب في أزمات سياسية وأمنية بين الدول بعضها بعضًا، لذا ففكرة التخزين الداخلي للبيانات، يقلل من الاعتماد على نظام الكابلات الضوئية، على الرغم من أنه لن يكون بتلك الفاعلية، ولن يحد من التهديدات الجيوسياسية المرتبطة بالمعلومات، ولكن تعتقد الدول أن اتباع وسيلة من شأنها أن تحد من تلك التهديدات، هو أمر مبرر في ظل هذا القلل المشروع بشأن النقل الخارجي للبيانات.(١٦)

٥. مواجهة متطلبات العولمة؛

تأتي العولمة لتزيل العوائق الحدودية بين الشعوب والأمم، وتستهدف الانفتاح العالمي غير المسبوق، وغير المحدود، لتناظر به الدولة القومية ذات السيادة الوطنية على أراضيها، فمتطلبات العولمة تستهدف الانفتاح الاقتصادي والتجاري بين الدول والمؤسسات الدولية، وهو ما يتطلب التدفق الحر للبيانات والمعلومات بمختلف أنواعها، سواء كانت شخصية أو حساسة أو تجارية او حتى أمنية، وهو ما اعتبرته العديد من الدول انتقاص لسيادتها على أراضيها من جانب، ومواطنيها من جانب ثانٍ، والفضاء السيبراني من جانب ثالث، لذا جاءت سياسات التوطين بمثابة الهدف لدحض مبادئ العولمة، وذلك لأن العولمة تضاد التوطين، الأولى من اشتراطاتها الانفتاح والتدفق الحر للبيانات، ولكن الثانية وفق اعتقاد الدول تستهدف المحلية، والتخزين المحلي، وتعزيز سيادة الدولة الوطنية، وتعزز من فاعلية الدولة القومية ذات السيادة، وعلى اعتبار أن اتفاقيات التجارة الدولية تستهدف مبادئ العولمة وتتبناها منظمة التجارة العالمية، لكن العديد من الدول كان لها صدى آخر بشأن مشاركة بياناتها مع الشركات العابرة للقوميات، وكان أبرزها الصين، حيث أصدر قرارات بمنع مشاركة بياناتها مع الشركات الأجنبية، وعلى غرارها جاءت قرارات إيران

بشأن التوطين لأجل السيطرة على منصات التواصل الاجتماعي كـ'Facebook'، وعلى الجانب الآخر قامت شركة 'IBM'، بإنشاء نحو "١٥" مركز للبيانات خارج حدود تواجدها، وذلك تحسبًا لإجراءات توطين البيانات، وبالتالي فإن القوى المختلفة المناهضة لفكر العولمة وجدت من إجراءات التقييد على منافذ تدفق البيانات، السبيل للنجاة وما تفرضه من سياسات فوضوية في بعض الدول.(١٧)

٦. الحفاظ على روابط المجتمع وقيمه؛

عادة ما تسعى الدولة إلى الحفاظ على تماسك المجتمع وتعزيز روابط الوحدة والألفة بين أفراده، بالإضافة للقيم الوطنية من الولاء والانتماء، ولما كانت التكنولوجيا قادرة على الوصول لكافة المعدلات العمرية، بدءًا من الأطفال مرورًا بالشباب ووصولًا لكبار السن، فهي قادرة على التسلل إلى نسيج المجتمع، وضرب روابطه وقيمه، كما أن التدفق الحر للبيانات يعرضها للوصول غير القانوني من قبل الأجهزة الأمنية الأجنبية، والتي قد تتربص بدولة بعينها من خلال استهداف أفراد المجتمع، وضرب تلك الروابط الاجتماعية، لذا سعت الدول لسياسات توطين البيانات لأجل الحفاظ على وحدة مواطنيها، من خلال الحفاظ على البيانات التي تخص الهوية، والكنية، كما أنها ضمنت وفق اعتقادها، تعزيز قيم الولاء والانتماء بالسيطرة الداخلية على خدمات الإنترنت والهاتف المحمول، التي قد يعرضها تخزين البيانات في الخارج للتهديد، وبالأخص أن الدول تقود حروب الجيل الرابع والخامس، والتي من خلالها تسعى للسيطرة على العقل البشري، وتوجيهه ضد معتقداته، وولائه وإيمانه بوطنه.(١٨)

ثانيًا الدوافع الأمنية؛

في هذا البند سيتم التطرق للدوافع الأمنية بشأن سياسات توطين البيانات، وأهمها حماية الأمن السيبراني، بالإضافة لحماية الخصوصية "أمن البيانات"، ويمكن تناولها على النحو الآتي؛

١. حماية الأمن السيبراني؛

حيث يعتبر الهدف الرئيس لتحقيق الأمن – السيبراني– في ظلال البيئة المعلوماتية والرقمية ممثلًا في؛ **أولًا ضمان السرية**، من خلال حماية خصوصية البيانات كونها تمثل أهمية كبيرة في عالم التكنولوجيا، وضمان السرية لا يتم فقط بحفظ الأسرار الداخلية للبيانات الشخصية أو الحساسة، ولكن كذلك ضمان عدم انكشاف العلاقة التي تجمع بين مالك البيانات ومزودي خدمات الإنترنت، ويتم تدعيمها من خلال العناصر التقنية؛ كبرامج التشفير أو إمكانية الوصول أو من خلال التشريعات القانونية، **ثانيًا تحقق النزاهة**، من خلال ضمان أن البيانات لا يتم استخدامها على نحو غير صحيح أو لأغراض غير التي جُمعت من أجلها، وأنها لم تتعرض للوصول غير المشروع وغير المقترن بإذن صاحبها، بمعنى هذا الهدف يتطلب الدقة والثقة ويعد جوهر أنظمة المعلومات لضمان نزاهتها ومصداقيتها، وكلما كان النظام المعلوماتي أكثر دقة كلما جذب المهاجمين والمخترقين، وكان أبرز نظام لهذا النموذج هجوم "Stuxnet' – الذي عبارة

عن دودة معلوماتية، تم صنعها لاستهداف أجهزة الطرد المركزية لتخصيب اليورانيوم في إيران ٢٠١٠، حيث أنها فيروس مخصص لقيام لجعل الأجهزة تدمر نفسها بنفسها، دون ملاحظة ذلك، كما أنه حظي بالاهتمام العالمي، كونه أول فيروس يتم تصنيعه لتعطيل أجهزة الكمبيوتر وجعلها تحرق ما بداخلها – [١٩]، على الأجهزة الإيرانية، وجاءت خطورته في جعل الأجهزة الإلكترونية تعمل بشكل طبيعي وعدم قدرة الأنظمة على اكتشاف هجومه، **ثالثًا الإتاحة أو التوفر**؛ أي إمكانية أن يتم استخدام الموقع على النحو الأمثل، على الرغم مما قد يترتب على التوفر من هجمات سيبرانية بالسيطرة على الأنظمة الإلكترونية فعليًا أو من خلال التهديد بفقدان الموقع كما يتم في الأنظمة البنكية أو الأنظمة الحكومية من خلال برامج يطلق عليها "الفدية" دون أيه معوقات، وبتحقق تلك الأهداف الثلاثة تعد ضمانة لحماية الأمن السيبراني للدولة، الذي يعد جانب من جوانب الأمن القومي للدولة.[٢٠]

فتلك الأهداف الثلاثة تمثل جوهر الأمن السيبراني – الذي يستهدف البنى التحتية التكنولوجية وحماية البيانات من الهجمات الضارة، بالإضافة لاستهدافه أي مجال متصل بالشبكة المعلوماتية، ويتم مشاركة البيانات من خلاله سواء كانت أمنية، معلوماتية، عسكرية، اقتصادية، سياسية، ثقافية، أو تجارية – ويطلق عليها "**ثالوث الأجهزة المخابراتية المركزية**"، لذا جاء الاعتقاد بأنه على الرغم من أن تلك الأهداف الثلاثة تضمن الأمن النسبي للأنظمة المعلوماتية، إلا أنها تجعلها مُعرضة للتهديدات السيبرانية، من خلال الهجمات الداخلية أو الخارجية، وهو ما كشفت عنه اكتشافات "سنودن" بأن الولايات المتحدة الأمريكية كان لها منفذ للوصول للبيانات تخطى بدوره حدودها الوطنية، بل وأضاف أن شركات 'google', 'yahoo'، قد مكنت وكالة الأمن القومي الأمريكية من الوصول إلى بيانات مستخدميها، لذا جاءت تدابير توطين البيانات لأجل حماية البيانات من الوصول غير المشروع، واعتبرتها بأنها ستحسن من البيئة السيبرانية مما يزيد من دعائم الحماية بها، وذلك لأن فكرة إنشاء مراكز لتخزين البيانات داخليًا وإنشاء شبكات إنترنت منفصلة عن الإنترنت العالمي، هو وفق تحليلات الدول سيضمن ألا تتعرض البيئة المعلوماتية لتهديدات الهجمات الإلكترونية المتكررة، وهو ما ترجمته دولة "ألمانيا"، عندما أطلقت مبادرة تنادي من خلالها الاتحاد الأوروبي بإنشاء شبكة إنترنت داخلية تخضع لرقابة وسيطرة الاتحاد الأوروبي لضمان عدم التجسس الأمريكي على البيانات الألمانية والأوروبية.[٢١]

وفي حين أن هنالك تحليلات تخدم أغراض التوطين لحماية الأمن السيبراني إلا أن هنالك تحليلات أخرى تقنية تعتقد أن التوطين سيوسع من الهجمات السيبرانية وبخاصة أن العديد من الدول المتبنية لتلك السياسات تعاني أنظمة البنى التحتية التكنولوجية الخاصة بها من ضعف وفتور تقني، وهو ما يعرض فكرة التخزين المحلي لمخاطر الاختراق السيبراني بشكل أكبر من تدفقها عبر الحدود الوطنية من جانب، وبصورة أكبر من الفائدة التي ستتحقق من التخزين وفق نسخ احتياطية محلية تحسن من أداء عنصر التوفر لأنظمة

المعلومات، بالتالي فكل قطاع متصل بشبكة الإنترنت فهو مُعرض للهجوم والنشاط الموسع للاحتيال السيبراني، وهو ما أكده مؤشر **الجريمة للهند** ٢٠٢١ حيث أشار أن المخاطر السيبرانية لم تتراجع أو تنتهي حدتها، على العكس فقد تضاعفت بنحو تسع مرات ٢٠٢٠ عن آخر رصد لها منذ ٢٠١٣، حيث أنه عام ٢٠١٣ سجلت حالات الجرائم الإلكترونية في الهند نحو ٥٦٩٣، وسجل عام ٢٠١٤ تزايدًا في عدد الجرائم المُبلغ عنها بنحو ٩٦٢٢ جريمة، وبلغت نسبة الارتفاع ٦٢٪ من إجمالي الأرقام المسجلة في سنة البدء "٢٠١٣"، وتصاعد هذا الرقم ليصل لنحو ١١٥٩٢ جريمة، والملاحظ أنه خلال عام ٢٠١٨ قد قفزت حجم الجرائم السيبرانية المرتكبة داخل الهند بنحو ٢٧٢٤٨ جريمة، بمعدل ارتفاع ٨٥٪ من إجمالي الجرائم التي تم الإعلان عنها، وهي قفزة واضحة في حجم تلك الجرائم على الرغم من تصعيد الدولة إجراءاتها بشأن تقييد البيانات، ولاسيما في ظل توجيه بنك المدفوعات من جانب، وإعلان الحكومة الهندية مسودة قانون حماية البيانات الشخصية.[٢٢]

وبرغم ذلك لم تتراجع معدلات الجريمة السيبرانية داخل الهند، بل تضاعفت أعدادها، لتسجل عام ٢٠١٩ نحو ٤٤٥٤٦ جريمة، وتوالت الزيادة بنحو ٥٤٨٩ جريمة، إضافة للعدد السابق لتصل لنحو ٥٠٠٣٥ جريمة، وسجلت قرابة ٥٢٩٧٤ جريمة عام ٢٠٢١، بزيادة إضافية عن العدد السابقة مقدارها نحو ٢٩٤١ حالة، لتعد هي الحد الأدنى للزيادة في حجم تلك الجرائم منذ عام ٢٠١٣، وهي تعد إيجابية برغم أنه انخفاض في معدل الزيادة لتسجيل تلك الجرائم، وأشارت تقديرات أخرى بأن تلك الجرائم كانت أغلبها في نطاق جرائم الاحتيال والابتزاز، وأن مستخدمي الإنترنت قد فقدوا قرابة ١٥ مليار دولار جراء تلك الجرائم ولاسيما عام ٢٠١٧، [٢٣] لذا عند الحديث عن الأمن السيبراني يتعين أن يتم تدعيم البنية التحتية التكنولوجية للدولة للحديث عن إجراءات توطين لحماية البيانات، وحماية بيئة المعلومات السيبرانية، ونظام الدولة الرقمي. [٢٤]

٢. حماية الخصوصية للمواطنين "أمن البيانات"؛

بالتطرق لمفهوم لخصوصية، يعني "حق الفرد في ألا يُنتهك الحيز الخاص به، بل وأن ينعم بالهدوء والسلام النفسي، وألا يشعر بأنه مخترق من قِبل الآخرين"، لذا فالحق في الخصوصية يضمن للفرد الدفاع عن مقدساته الشخصية من الانتهاك والتعدي غير المبرر، وإذا كان الباحث بصدد تناول الخصوصية من منظور البيانات، فهي تعني البيانات الشخصية للفرد التي يشاركها مع مقدمي خدمات الإنترنت، لأجل التمتع بخدمات الحوسبة السحابية، لذا فتعتقد العديد من الدول أن فكرة انتقال البيانات الشخصية للفرد عبر الحدود الوطنية، ما هو إلا انتهاك لخصوصيته بالإضافة لأنه يشكل اختراق لهوية المجتمع في الداخل، لذا فجاء اتباع سياسات توطين البيانات ظنًا منها أنه بتخزين البيانات في الداخل سيحفظ خصوصية المواطنين، فضلًا عن أنه يعزز تدابير أمن البيانات ظنًا منهم أن التخزين بالداخل لن يعرضها للمخاطر

السيبرانية، وبالتالي فإن الحق في حماية الخصوصية المعلوماتية للأفراد إنما هو إيذانًا للفرد في التحكم في الغرض الذي تُجمع من أجله بياناته، والنطاق الزمني التي تستهدفه، بالإضافة لسُبل معالجتها، أي أنه يجعله المتحكم في مصيرها، وهو ما يمكن أن يطلق عليه حق تقرير المصير المعلوماتي للفرد، كما جاء في نظرية "تقرير المصير للمعلومات الشخصية" التي تتيح بدورها للفرد كامل الحق في إدارة توجهات بياناته.[٢٥]

أضف لذلك أن انتهاج تدابير التوطين، سيسمح بالتخزين الداخلي وفق اعتقاد الحكومات، والذي سيسمح بقيام الدولة بمهام الحماية والمراقبة الداخلية، بالتالي فهي اعتمدت على فكرة المكان كأساس لحماية الخصوصية وأمن البيانات، ويلاحظ فعليًا أن هنالك دول اتخذت إجراءات بشأن حماية المعلومات الشخصية والخصوصية، من خلال إصدار تشريعات عدة، ومن أبرزها إندونيسيا، وكوريا الجنوبية، بالإضافة لقيام الهند ممثلة في بنك الاحتياط الهندي، بتوجيهات لمزودي خدمات الدفع الإلكترونية بإنشاء مراكز لتخزين بيانات الدفع داخل الهند لتنتهي عام ٢٠١٨ الماضي. [٢٦]

وبالتدقيق فيما اعتمدته تلك الدول لتبني سياسات التوطين، يتضح أنها اعتمدت على مكان التخزين لتوفير الخصوصية، ولكنها أهملت الجانب التقني والفني، بمعنى هل تركيز البيانات في موقع واحد للتخزين لن يعرضها للهجوم السيبراني من قِبل مخترقي النظام الرقمي، أضف لذلك هل تمتلك الدول البنية التحتية التكنولوجية لاستضافة بيانات مواطنيها وتوفير معايير متقدمة لحمايتها؟، فهنالك العديد من الدول التي تعاني أنظمة البنى التحتية التكنولوجية لها من افتقار لعنصر الدقة والتقدم المعلوماتي والأمني، وبالتالي لا تعد جاهزة لتلك المسئولية، وذلك لأنه إذا ما تمت المقارنة فالشركات العالمية مُقَدِمة تلك الخدمات تتمتع بمستوى متقدم من التنافسية وهو ما يفرض عليها البقاء في سوق التكنولوجيًا، لذا فإنها تتبع معايير أمنية دقيقة للغاية، وتستعين بأنظمة تشفير معقدة لا يتم اختراقها بتلك السهولة، وأخيرًا فكرة المركزية في التخزين تقضي على الميزة التي تتمتع بها شبكة الإنترنت العالمية وهي "التجزئة"، حيث أن تلك السمة تعطي للشبكة المعلوماتية القدرة على تجزئة البيانات من خلال قواعد تخزين البيانات المختلفة، وهو ما يحد من فرص اختراقها والوصول لها، لكن فكرة التوحيد المعلوماتي يسهل من عمل اللجان الإلكترونية في الوصول لتلك البيانات، ومنه إلى اختراق الخصوصية، كما أن فكرة التوطين للحفاظ على سرية البيانات أي خصوصيتها هو بالأمر غير المنطقي، لأن ضمان السرية غير مرتبط بتغيير مكان التخزين ولكنه يتعلق بالأنظمة المستخدمة في التخزين، إضافة للجوانب الفنية والتقنية كنظام التشفير أو إخفاء الهوية أو التسمية المستعارة، وعناصر الخبرة المعلوماتية، فسرية البيانات في خادم خارج الدولة ذاتها في خادم داخل الدولة، بل أنها قد تكون معرضة داخليًا للانكشاف لعدة اشتراطات من ضمنها مظلة الأمن القومي، بالتالي فربط الحفاظ على السرية باتباع التوطين هو أمر يتطلب إعادة التدقيق في مضمونه وأبعاده.[٢٧]

هنالك جانب آخر سياسي مرتبط بفكرة الخصوصية، تُجْادل العديد من الدراسات بشأن أن هذا الدافع إنما هو رغبة من قِبل الأنظمة السياسية وخاصة الاستبدادية منها، لمراقبة مواطنيها، والتعدي على حقوق الخصوصية لديهم، ومنه للسيطرة على كافة المرافق الإلكترونية لمراقبة ما يتم تداوله على الشبكة الافتراضية، لكبح المعارضة، وتقويض الحريات، بما فيها حرية التعبير عن الرأي، وحجب المواقع غير المرغوبة والتي تعتبرها الدولة مهددة للأمن الوطني والاستقرار الداخلي، كقيام الصين بإنشاء مشروع "**Golden shield**" أو الجدار الناري للصين العظيم، والمختص بمراقبة شبكة الإنترنت وحجب المواقع غير الموثوقة، واطلاق أخرى بديلة خاضعة لسيطرة ورقابة الصين كمحرك البحث "بايدو"، وموقع "ويبو" للنشر القصير،[٢٨] إضافة لحالات الإغلاق لشبكة الإنترنت في الهند والذي أظهر أن الهند كانت صاحبة النصيب الأكبر في إغلاقات الإنترنت بنحو ١٠٦ مرة خلال عام ٢٠٢١، كما أصدرت شركة فيسبوك تقريرًا عام ٢٠١٣، لتشير من خلاله أن الهند قامت بطلب بيانات لمستخدمين هنود لتطبيق الفيسبوك، بلغت نحو ٣٢٤٥ طلب. [٢٩]

٣. مكافحة قضايا الإرهاب وغسيل الأموال؛

على الرغم من حقيقة أن التدفق اللانهائي للبيانات عبر شبكة الإنترنت، قد أتاح الاتصال والتواصل بين مختلف الأفراد في شتى بقاع الأرض، بطرق ميسورة، لا تتسم بتلك التكلفة المرتفعة، وأدى بدوره إلى ارتفاع الطموحات الدولية بشأن شبكة الإنترنت العالمية، للاستفادة منها في مجال تبادل المعلومات والبيانات التي تخدم أغراض التجارة الرقمية، والتسوق اللامحدود، إلا أنه فرض العديد من التحديات على الأجهزة الأمنية الوطنية، حيث أنه بدأت عملية الاستغلال غير القانوني لشبكة الإنترنت بما تتضمنه من سيل من البيانات والمعلومات المتنقلة وغير الخاضعة لسيطرة ورقابة الدول، وجاءت الصور غير المشروعة لاستخدام الإنترنت، فيما يتعلق بالترويج للفكر المتطرف والأعمال غير المشروعة كالإرهاب والاحتيال المالي، فعن الإرهاب فقد تم استغلال إتاحة المعلومات في الدعاية والترويج للعنف والكراهية، ونشر الفكر المتطرف، وأعمال التجنيد للأهداف المباشرة، وذلك من خلال الهجمات الإلكترونية التي يشنها المخترقين التابعين لتلك التنظيمات بغرض الاستيلاء على البيانات والمعلومات الشخصية أو السرية لأجل دراسة الهدف والتخطيط لعملية تجنيده من خلال استهداف فكره ومعتقده وآراءه السياسية إن تطلب الأمر، وجدير بالذكر أن تلك الهجمات قد ازدادت بنسبة ١٣٦٪ خلال عام ٢٠٢١ في مختلف أنحاء العالم، وكان أغلبها في نطاق الاحتيال والوصول للبيانات والمعلومات الشخصية، فشهد عام ٢٠٢١ وقوع قرابة ٣٢٣،٩٧٢ مستخدم للاحتيال الإلكتروني، كما تم تعرض قرابة مليار رسالة بريد إلكتروني للوصول غير المشروع وكشف ما بها من بيانات خلال نفس العام كذلك، وكانت أكبر الدول تأثرًا بتلك الهجمات الإلكترونية المملكة المتحدة بزيادة مقدارها ٤٠٪ في حجم تلك الجرائم عن عام ٢٠٢٠. [٣٠] أما عن الاحتيال المالي، فتمثل كذلك في

استغلال الأموال غير المشروعة لأعمال تمويل الإرهاب، وغسيل الأموال، للتستر على خلفية مالك تلك الأموال وأنشطته المختلفة،[٣١] فخلال عام ٢٠٢١ ارتفع متوسط درجة مخاطر جرائم غسيل الأموال من ٥.٢٢ عام ٢٠٢٠ لنحو ٥.٣ من إجمالي تقييم ١٠ وفقًا لمؤشر بازل السويسري لمكافحة غسيل الأموال، كما بلغت إجمالي الغرامات المفروضة على جرائم غسيل الأموال إجمالي ٢٢ مليار دولار عام ٢٠٢٠، وانخفضت لتصل لنحو ٩ مليار دولار عام ٢٠٢١، كما بلغت إجمالي متوسط الأموال التي تم غسلها في الولايات المتحدة الأمريكية عام ٢٠٢٠ نحو ٣٠١ مليار دولار، كما تبلغ خسائر المملكة المتحدة من جرائم غسيل الأموال قرابة ١٣٦ مليار دولار أي ما يمثل ١٤.٥٪ من الناتج المحلي للمملكة المتحدة. [٣٢]

لذا اعتبرت العديد من الدول أن هذه الإتاحة للبيانات وتدفقاتها المفتوحة عبر شبكة الإنترنت، إنما تمثل ناقوس من شأنه أن يعرض الأمن الوطني للخطر، وتحديدًا من خلال استغلال الأفراد داخليًا لأعمال العنف والتطرف، وتحويلهم لخلايا نائمة لخدمة تنظيمات بعينها، من خلال التواصل السري عبر أنظمة إلكترونية مشفرة بمعايير جودة عالية، حتى لا يتم تتبع المواقع الصادر منها الإشارات، واعتمدت الدول تلك الحُجة لأجل تقييد انتقال البيانات عبر الحدود، وذلك تحت مظلة السيطرة على المعلومات، وتمكين إنفاذ القانون وجهات التحقيق من الحصول على المعلومات الكافية بشأن الأنشطة المشبوهة حتى يتسنى الكشف عنها والحد من تهديداتها هذا من جانب، أما الجانب الآخر مرتبط بإنشاء هيئات أمنية إلكترونية تتمثل مهامها في مراقبة وسائل التواصل من أجل اكتشاف أعمال التحريض غير القانونية على الشبكة، ولأجل مكافحة الإرهاب الإلكتروني ومحاصرة عمليات التمويل الافتراضية لتلك الأعمال.

ولكن بالرغم من ذلك اعتقد الكثيرين أن تدفق البيانات غير المحدود يتيح للأجهزة الأمنية العالمية تبادل المعلومات فيما بينها بشأن جرائم الإرهاب والفساد المالي، وبالتالي تسهم في مساعدة أجهزة التحقيقات الدولية، وأن عملية التقييد من شأنها أن تحد من إمكانية التبادل الحر للمعلومات بين الجهات الأمنية، مما يعرض مصير التعاون الأمني الدولي بشأن الجرائم العابرة للحدود لتحديات الانتشار وتوسيع النشاط، والاستهداف الحرج لشخصيات بعينها.

ثالثًا الدوافع الاقتصادية "تعزيز الاقتصاد القومي"؛

تأتي الدوافع الاقتصادية على قمة أولويات الدول المتبنية لسياسات توطين البيانات، وذلك بغرض دعم التنافسية للاقتصاد المحلي في قطاع تكنولوجيًا المعلومات والاتصالات، في مواجهة الشركات متعددة الجنسيات، حيث إنه وفق اعتقادها، سيمُكن الشركات المحلية من التنافس في قطاع التكنولوجيا على مراكز تخزين البيانات، مما سيعود بدوره على انخفاض معدل البطالة، وزيادة معدلات العمل داخل الدولة، كونه سيتم نقل الوظائف المرتبطة بالبيانات إلى داخل الدولة، وتعزيز الإنتاجية المحلية، لكسر الاحتكار الأجنبي لسوق التكنولوجية المحلية، ولعل ما يدعم من هذا التبني أن مراكز تخزين البيانات في العديد من الدول

تُسهم في آلاف الوظائف للأفراد المتخصصين في هذا المجال، [٣٣] حيث ساهمت بنحو ٤٥٠٠٠ وظيفة للأفراد في ولاية فرجينيا في الولايات المتحدة الأمريكية، كما أن احتمال إنشاء مركز لتخزين البيانات محليًا يجعل من المحتمل أن يخلق ما بين ٢ إلى ٣.٥٤ وظيفة لكل فرد، بالإضافة لتشجيع الصناعات المحلية الناشئة، وعدم الطلب المُلح على العملات الأجنبية لدفعها لمزودي الخدمة نظير تخزين بيانات مواطنيها، وهنالك سبب آخر مفاده أنه سيعزز من البنية التحتية التكنولوجية، وليخلق فرصة للشركات الناشئة للمنافسة على تقديم خدمات الإنترنت، وطلب التخزين المحلي للبيانات، وجاءت تقديرات اقتصادية بأنه متوقع زيادة الطلب على خدمات **مراكز التخزين في الهند** لتنمو بنحو ٢٥٪ وترتفع من ٢ مليار دولار إلى ٥ مليار دولار بحلول عام ٢٠٢٣. [٣٤]

والاستثمار في قطاع التكنولوجيا، مما ينعكس بدوره إيجابًا على فرص الابتكار تعزيزًا لمفهوم الاقتصادي القومي، فعلى سبيل المثال يحقق الاقتصاد الرقمي في الهند نحو ٢٠٠ مليار دولار سنويًا، ومتوقع أن ترتفع قيمة إيراداته بفعل سياسات التوطين لنحو تريليون دولار عام ٢٠٢٥ وذلك على الرغم من أن فكرة التوطين لتعزيز الاقتصاد المحلي لاقت الانتقاد لعدد من الأدبيات، وذلك باعتبار أنها ستصيب الاقتصاد المحلي بأضرار وذلك لارتفاع تكاليف الخدمات المقدمة من قِبل الشركات العاملة، كما أنها ستقضي على التنافسية المحلية لصالح الشركات النافذة والمتقدمة في الصناعة، وأن الشركات الناشئة ستتعرض للمخاطر الأمنية لأنها لا تمتلك التمويل الكافي لتعزيز بنيتها التحتية وسُبل أمانها، كما أنها لا تمتلك خبرات الشركات النافذة لمجابهتها في سوق العمل الرقمي، بل أنه سيؤثر على خدمات إنترنت الأشياء المرتبط بالتجارة الإلكترونية المعتمدة على سيولة البيانات، التي يعتبرها خبراء الاقتصاد بأنها منفعة للعامة وتقييد تدفقها سيؤدي إلى تحجيم أدوات التنمية المستقبلية.[٣٥]

رابعًا الدوافع التكنولوجية؛

تأتي الأهداف التي أعلنتها بعض من الدول في هذا الملف ما يتناسب ومتطلبات تعزيز صناعة التكنولوجيا محليًا، بالإضافة إلى بناء شبكات معلوماتية محلية مستقلة تنفصل بدورها عن شبكة الإنترنت العالمية، تستهدف كافة الأنشطة المحلية فقط، هذا بالإضافة إلى تعزيز البنية التحتية التكنولوجية المحلية، لأنها تسهم في خفض تكاليف الخدمات التكنولوجية المُقَدَمة، كما أن هنالك هدف آخر للملف التكنولوجي موصول مع الملف السياسي، مرتبط بمنع الوصول غير المشروط إلى البيانات، وذلك لحماية المعلومات من مخاطر الرقابة الأجنبية، أضف لذلك اعتماد أنظمة تشفير متشعبة، بمعنى إن اتجاه الدول نحو التوطين، سيتعين عليها اتباع أنظمة تشفير متشبعة غير متماثلة وليست متماثلة لأجل ضمان حماية البيانات من الوصول الأجنبي لها، لأنها تتسم بالتعقيد، ولكن بالنظر إلى جملة ما تم تداوله من دوافع فإنها تتضمن البعد التكنولوجي كذلك، فعند تناول الأمن السيبراني كدافع أمني فإنه ينطوي على دافع تكنولوجي لأجل

حماية الأمن الإلكتروني، وتعزيز بناء الشبكة، وحماية نظام المعلومات الداخلي، ومنع استغلال البيئة المعلوماتية المحلية في أغراض غير قانونية، وهذا جوهر التكنولوجيا، كما أنه عند التطرق لتعزيز التنافسية المحلية الاقتصادية، فكانت مرتبطة أساسًا بصناعة التكنولوجية، لذا فهذا الدافع متداخل مع الدوافع الاقتصادية، السياسية، والأمنية كذلك.

ويخلص مما سبق، أبرز ما تناوله هذا المطلب، الدوافع المختلفة لتوطين البيانات، والتي كان من أبرزها إنفاذ القانون، وتعزيز السيادة الوطنية في صورتها الرقمية، بالإضافة لتعزيز الأمن السيبراني، وحماية الخصوصية، ولكن بالنظر إلى ما تنضوي عليه الدوافع السياسية، فإنها أداة حادة ذات وجهين، فمن الجانب الذي تسعى به لتضمن أمن البيانات، ظهر جانب آخر أكثر حُجة وقوة في ادعاءاته، بأنها لتفرض الدولة سيطرتها على المعلومات ومراقبة محتوى ما يتم تقديمه للأفراد على المنصات الإلكترونية، كما أنه أداة فعالة للأنظمة الحكم التقييدية لأن تُحَجم من تأثير المعارضة، من خلال الاضطلاع على البيانات الخاصة بهم ومراقبة نشاطاتهم على شبكات التواصل الاجتماعي، بل أنها قد تكون أداة لقمع الحريات وحقوق الإنسان، ولاسيما فيما يخص المجتمعات المتمايزة عرقيًا وطائفيًا، كما أنه من الممكن أن يكون التوطين لغرض منع الوصول غير المشروط للبيانات من قبل الدول الأجنبية؛ أداة بيد الحكومة لتفعل الوصول المحلي غير المشروط كذلك على بيانات مواطنيها، وكأنها للتخلص من الاستعمار الرقمي الأجنبي، استعانت بالاستعمار الرقمي المحلي.

المحور الثالث؛ الاشتراطات والمتطلبات لتبني سياسات توطين البيانات.

يأتي هذا المحور ليتم من خلاله تناول الاشتراطات والمتطلبات لتبني سياسات توطين البيانات في الدولة، والتي تختلف من دولة لأخرى وفقًا لنوع التوطين المتبع، فسبق أن تمت الإشارة لتصنيفات التوطين؛ الصارم، المختلط، الناعم، والواقعي، لذا فعند الحديث مثلًا عن متطلبات التوطين الصارم، فتشترط التخزين والمعالجة الداخلية للبيانات المحلية كما في نموذجي الصين وروسيا، في حين أنه إذا تمت الإشارة إلى النوع الثاني، فمتطلباته، تشترط أن يتم السماح بالتخزين الخارجي لأغراض المعالجة فقط، ولكن مع حذف البيانات عقب ٢٤ ساعة من المعالجة، مع احتفاظ الدولة الوطنية بنسخة داخلية، ويمثله قرار بنك الاحتياط الهندي الذي طالب بأن يتم تخزين بيانات المدفوعات ومعالجتها داخل الدولة، ومنع انتقالها للخارج لذات الغرض، أما بالنظر لمتطلبات التوطين الناعم، فإنها لا تشترط التخزين والمعالجة الداخلية بل أنها تسمح بانتقالها للخارج لذات الهدف، مع احتفاظ الدولة بنسخة احتياطية من تلك البيانات، وأخيرًا عن متطلبات التوطين الواقعي، فإنها تتطلب الامتثال لتدابير بعينها، واستيفاء معايير أمنية تحددها الدولة لأجل السماح بانتقال البيانات للمعالجة والتخزين سواء في بلد مزودي الخدمة أو دولة أخرى اجنبية محل ثقة متبادلة مع

أطراف التوطين، لذا عند النظر في باطن الأمر يتضح أن هنالك عنصرين مشتركين في المتطلبات وفقًا لنوع التوطين ألا وهما؛ متطلبات التخزين، ومتطلبات المعالجة، ويمكن تناولها كما والتالي؛[٣٦]

١. **متطلبات التخزين**؛ عادة ما تشترط الدول من خلال سياسات توطين البيانات، متطلبات بعينها لتخزين البيانات في مراكز محلية داخل حدود الدولة، قد تكون فئة معينة من البيانات التي تفرض التقييد عليها، كالبيانات الشخصية والحساسة أو فئات متعددة من البيانات الحكومية أو التجارية، وفقًا لدرجة الأهمية والحساسية، وتتراوح متطلبات التخزين ما بين التقييد الكامل بمنع انتقال البيانات أو التقييد مع السماح بالانتقالات.

٢. **متطلبات المعالجة**؛ وهي ما تتضمنه من إجراءات وتدابير وخطوات يتم تطبيقها على البيانات لمعالجتها، وفقًا للهدف الذي أنشأت من أجله، بمعنى معالجتها لتلبي معايير الخدمة الإلكترونية، فتحويل الرموز والنصوص والأرقام إلى نصوص مقروءة ومفهومة قابلة للاستخدام الإلكتروني والرقمي وإدارتها على النحو الأمثل لتحقيق الاستفادة منها، تلك هي جوهر عملية المعالجة، لذا فإن إجراءات توطين البيانات تفترض متطلبات للمعالجة، إما أن تكون معالجة محلية فقط داخل مراكز بيانات تخضع لسيطرة ورقابة الدولة أو السماح بمعالجتها خارج حدود الدولة وفق اشتراطات محددة.

هنالك نماذج مختلفة لتمثل الدرجات المتفاوتة لمتطلبات التوطين، منها؛ **أولًا الصين**، حيث تأتي متطلبات التخزين لديها وفقًا لقانون الأمن السيبراني الصيني بالتعامل المحلي مع البيانات الصيني، من خلال مراكز بيانات صينية، وهو ما يفترض نطاق أوسع لمتطلبات التخزين، حيث أنه قديمًا كانت الصين تحظر نقل نوع معين من البيانات للخارج بغرض التخزين كتلك المستهدفة أسرار الدولة العميقة، وأخرى مرتبطة بالبيانات المالية والصحية، وتسمح لبقية البيانات بالسيولة والانتقال الحر للخارج للتخزين، لكن بصدور قانون الأمن السيبراني، فرضت متطلبات صارمة للغاية استهدفت أغلب البيانات الصينية، حتى تلك التي يتعين أن تنتقل للدواعي التجارية والاقتصادية فإنها تعود لمراجعة السلطات الأمنية الصينية والتي في غالب الأمر ترفض النقل لاعتبارات الأمن القومي، [٣٧] **ثانيًا روسيا**؛ تأتي متطلبات التوطين وفقًا للقانون الاتحادي الروسي، لتمثل النوع الصارم منها كما والصين، حيث اشترط القانون بأن تكون جميع مراكز البيانات التي تحتوي البيانات الشخصية للمواطنين الروسيين داخل الأراضي الروسية، بل وأن يتم الامتثال من قِبل الشركات الأجنبية لتدابير التوطين بأن يتم التعامل من خلال الشبكة الروسية المحلية 'RUnet'، وبمدخلات اللغة الروسية، **ثالثًا الهند**؛ تشمل متطلبات التوطين لديها شقين، الأول متطلبات التخزين الخارجي المُيَسر للتخزين والمعالجة في حين الاحتفاظ بنسخة داخل الهند، وذلك على كافة أنواع البيانات، في حين أن الشق الثاني؛ يأتي بتقييد نوع محدد من البيانات بتخزينه داخل حدود الدولة، كنظام المدفوعات الهندي، ولكن السماح له بالانتقال الخارجي للمعالجة فقط.[٣٨]

رابعًا الاتحاد الأوروبي؛ فرضت اللائحة العامة لحماية البيانات 'BGDR'، بمتطلبات محددة على عملية انتقال البيانات خارج حدود الاتحاد الأوروبي، حيث اتاحت الانتقال للتخزين والمعالجة باشتراطات توفير معايير متقدمة ومعقدة للأمن والحماية السيبرانية لتلك البيانات أو أن يتم نقلها لدولة أجنبية ثالثة تتوفر فيها معايير الأمن والخصوصية التي يقرها الاتحاد الأوروبي، كما أنها قامت بعمل نموذج لمراكز البيانات داخل الاتحاد الأوروبي ضمن مبادرة ألمانيا لمنطقة "شنغن"، وذلك لضمان معايير التخزين والحماية للبيانات الحساسة غير القابلة للانتقال خارج حدود الاتحاد الأوروبي، **خامسًا فيتنام؛** جاءت متطلبات التوطين وفق مشروع قانون الأمن السيبراني بالتخزين الداخلي لكافة بيانات المواطنين، وجاء مرسوم "٧٢" لشمال فيتنام ليقر متطلبات أخرى أكثر صرامة للتوطين، بأن يحق للسطلات الأمنية الفيتنامية بمراقبة المحتوى الذي يُقَدَم عبر شبكات التواصل لأجل الحفاظ على استقرار الدولة وضمان استمرارية المبادئ والمُثل الأخلاقية، والاحتفاظ بنسخة من بيانات المواطنين كذلك، بل وصل الأمر لحجب مواقع بعينها أو أفراد إذا ما ثبت تورطهم في أعمال تهدد أمن الدولة وتسعى لهدم نظامها، **سادسًا نيجيريا؛** أقدمت على اشتراطات عقب تسريبات "سنودن" ديسمبر ٢٠١٣ بأن يتم تخزين كافة البيانات الشخصية للأفراد والمستهلكين، بالإضافة للبيانات الحكومية النيجيرية المرتبطة بخدمات الاتصالات وتكنولوجيا المعلومات داخل حدود نيجيريا.[٣٩]

سابعًا أستراليا؛ تأتي متطلبات التوطين لديها بشأن تقييد نوع واحد من البيانات والخاص بملف الصحة، حيث اشترطت التخزين المحلي له، **ثامنًا تركيا؛** أصدرت قانون على المدى البعيد يستهدف تخزين بيانات الدفع الإلكتروني داخل الأراضي التركية. [٤٠]

لذا ومن خلال ما سبق طرحه فيما يتعلق بمتطلبات التوطين المُتَبعة وفقًا لكل نوع على حدة يمكن استخلاص **الاشتراطات** الواجب توافرها، لتطبيق سياسات توطين البيانات؛

- بنية تحتية معلوماتية متقدمة لأجل استقبال البيانات وتوفير الحماية والخصوصية لها.
- خوادم أو مراكز تخزين للبيانات داخلية تخضع لرقابة وسيطرة الدول.
- تقييد نقل البيانات عبر الحدود الوطنية في حالة التوطين الصارم، والنقل المشروط في حالة التوطين الواقعي، والنقل مع توفير النسخ الاحتياطية في حالة التوطين الناعم، والنقل للمعالجة مع التخزين الداخلي في حالة التوطين المختلط.
- الاستعانة بأنظمة حماية متقدمة ومعقدة يصعب اختراقها كما وأنظمة التشفير.
- تشريعات قانونية نافذة وفعالة تضمن التطبيق الفعلي لسياسات التوطين وتحديد الضوابط القانونية لمخالفي تلك السياسات.

الخاتمة:

سبق أن تمت الإشارة خلال الدراسة إلى؛ الدوافع المحتملة لتبني العديد من الدول لسياسات توطين البيانات من خلال المحور الثاني، وقُسمت إلى **دوافع سياسية**، تضمنت مفهوم السيادة الوطنية، وإنفاذ القانون المحلي والامتثال القضائي، إضافة إلى مجابهة التدخلات الخارجية في شئون الدولة من خلال منع الوصول الأجنبي غير القانوني للبيانات، والحد من التهديدات الجيوسياسية المرتبطة بخدمات الموقع الجغرافي، هذا بالإضافة للحفاظ على قيم المجتمع وروابطه من خلال منع التسلل إلى نسيج المجتمع بالمحافظة على البيانات الشخصية للأفراد، وتعزيز قيم الولاء والانتماء، كما تم التطرق كذلك لدافع مواجهة متطلبات العولمة من الانفتاح والسيولة المعلوماتية، وعن **الدوافع الأمنية** فتمثلت في؛ حماية الأمن السيبراني، وحماية حقوق الخصوصية، بالإضافة إلى مكافحة قضايا الإرهاب والاحتيال المالي، وعن الدوافع التكنولوجي فقد تم ذكر الاستقلال الشبكي، فضلًا تعزيز البنية التحتية التكنولوجية، والإسهام في تشجيع الابتكار التقني والمعرفي، أما عن **الدوافع الاقتصادية** فتمثلت في؛ تعزيز التنافسية المحلية وبالأخص الشركات الناشئة في قطاع التكنولوجيا، لأجل تعزيز صناعة التكنولوجيا محليًا وانعكاسه على مستوى الخدمات وتكلفتها بالانخفاض، وكانت تلك الدوافع وفق ما تعتقده الحكومات وتعلنه صراحة.

ولكن بالوقوف عند تلك النقاط الهامة، وبالتحليل المنطقي، هنالك عدة إشكاليات، تمخضت عن تلك الدوافع، ويتعين الإشارة لها، وتتمثل في؛

فيما يتعلق **أولًا بالدوافع السياسية**، في البند المرتبط **أولًا بالحفاظ على السيادة الوطنية للدولة** في صورتها المعاصرة المرتبطة بالمعلومات، هل مفهوم السيادة يتحقق فقط عند انتقال البيانات من الصورة العالمية في التخزين إلى الصورة المحلية، داخل حدود الدولة، فما هو التوصيف لمفهوم السيادة في حال تعرضت تلك البيانات وفق تخزينها الداخلي للهجمات السيبرانية، وتم اختراق البيانات في أماكن تخزينها الداخلية؟، فهل السيادة الوطنية للدولة تتحقق فقط بإغلاق الدولة حدودها التقليدية والافتراضية على تلك البيانات، أم أنه يتحقق بمقدار ما تتخذه الدولة من تدابير لتحمي مقدراتها من تعرضها للاختراق والتعدي، ففكرة الحماية تعزز من مفهوم السيادة بدلًا من البلقنة والتخزين المحلي، لذا فهنالك إشكالية فعالية المفهوم في حال تم اتخاذ إجراءات التوطين لمتطلبات المعالجة والتخزين فقط دون البحث عن التدابير الفنية للحماية الفعلية لتلك البيانات، لأن التهديد بالاختراق تتعرض لها المعلومات المخزنة داخليًا بصورة أكبر من الخارجية، وذلك لأن الداخلية لا تعتمد التجزئة في التخزين، على عكس الخارج يعتمد التجزئة لأكثر من قاعدة بيانات، وبأنظمة تشفير معقد.

ثانيًا البند المرتبط بإنفاذ القانون المحلي، كما سبقت الإشارة يأتي التوطين لأغراض إنفاذ القانون ومساعدة أجهزة التحقيقات داخليًا للتحقيق في الجرائم المرتبطة بالبيانات والمعلومات الإلكترونية، ومعنى

أن يتم تقييد تدفق البيانات لصالح الجانب المحلي، فهنالك إشكالية التعاون الدولي في قضايا الإرهاب الدولي والاحتيال المالي، والجرائم المنظمة، التي تتطلب التعاون بين الجهات الأجنبية لتبادل وتدفق البيانات والمعلومات حول المشتبه بهم في تلك الجرائم ولاسيما إذا ما كانوا ينتموا لعدة الدول، فما مصير التعاون الأمني والمعلوماتي الدولي في ظل منع انتقال للبيانات للخارج أو الحد من انتقالها إلا باشتراطات غالبًا ما تخضع لرؤى وتوجهات الأنظمة الأمنية المحلية؟، ما مدى تأثر مكافحة الإرهاب الدولي، هذا ما سيتم قياسه خلال المبحث القادم.

ثالثًا البند المرتبط بالحد من الوصول الأجنبي للبيانات، برزت إشكالية وفقًا لهذا الدافع، هل فكرة انتقال مكان التخزين من الخارج للداخل، سيعزز من عدم الوصول الأجنبي للمعلومات والبيانات؟، كيف يمكن للدولة أن تقيس هذا الأمر، وعلى أي أساس اعتمدت في تحليلها على هذا العنصر، فإذا منعت الدول الوصول المباشر للبيانات من مراكز تخزينها الخارجية، فكيف لها أن تمنع الوصول غير المباشر للأجهزة الأمنية والاستخباراتية الأجنبية، التي تعتمد برامج عالية الدقة والتعقيد، حيث تضرب عمق الأجهزة المعلوماتية داخليًا دون أن يتم اكتشافها مسبقًا، أو حتى كيف للدولة ستضمن عدم الوصول الأجنبي للبيانات في ظل اعتماد صناعتها التكنولوجية على المنتجات الأجنبية والتي قد تمثل في حد ذاتها تهديد للبنية التحتية المعلوماتية للدولة.

ثانيًا الدوافع الأمنية، تمثلت الإشكالية في البند المرتبط **بحماية حقوق الخصوصية**؛ برزت إشكالية حقوق الإنسان في ظل هذا الدافع، وذلك إذا ما كانت تسعى الدول لتقييد انتقال البيانات عبر الحدود المحلية لحماية البيانات من الاستخدام غير العادل من قبل مزودي الخدمة، فكيف تضمن حقوق مواطنيها على البيانات الخاصة في ظل سيطرة البيانات والرقابة عليها، بل ومراقبة بعض مواقع التواصل الاجتماعي، فما هو مصير ملف حقوق الإنسان، وحريات التعبير في ظل التخزين الداخلي الخاضع للرقابة الداخلية من الأجهزة الأمنية؟

ثالثًا الدوافع الاقتصادية، فتمثلت الإشكالية في البند المرتبط **بتعزيز الاقتصاد المحلي**؛ تسعى الدولة من خلال تدابير التوطين لأن تعزز المنافسة المحلية بين الشركات العاملة في مجال التكنولوجيا، لكنها غضت الطرف على عدم كفاءة المنافسة، حيث أن تلك الناشئة لا تمتلك التمويل الكافي لتعزيز بنيتها التكنولوجية لمواكبة التقدم الذي تحققه الشركات الفاعلة في هذا المجال، وبالتالي ستكون المنافسة بالإيجاب لصالح الشركات الفاعلة، وهو ما سيؤدي إلى ارتفاع تكاليف الخدمة المقدمة للمواطن، **رابعًا الدوافع التكنولوجية**، تمثلت الإشكالية في البند المرتبط **بتعزيز البنية التحتية التكنولوجية**؛ برزت إشكالية الدول التي تعاني بنيتها المعلوماتية من الضعف، بل أنها مُعرضة للتهديدات السيبرانية باستمرار، فما هو مصير تلك الدول في حال انتهاجها سياسات التوطين هذا من جانب، أم الجانب الآخر المرتبط بدافع البنية التحتية

التكنولوجية، كيف يكون هدف الدولة تعزيزها بانتهاج التوطين في حين أنه من اشتراطات التوطين أن تمتع الدولة ببيئة معلوماتية قوية قادرة على التصدي للمخاطر المحتملة، فهنالك تناقض بين سعي الدولة لتعزيزه وبين أن شرط اتباع تلك السياسات أن تكون تتمتع فعليًا ببيئة معلوماتية متقدمة.

نتائج الدراسة؛

خلصت الدراسة لعدد من النتائج من خلال ما سبق عرضه من محاور يأتي أهمها على النحو الآتي بيان؛

١. استهدفت الدول سياسات توطين البيانات لأجل الحفاظ على السيادة الرقمية للدولة بالنظر في جغرافية مكان التخزين والمعالجة دونما النظر للجوانب الفنية والتقنية المرتبطة بعملية المعالجة والتخزين.
٢. استهدفت العديد من الدول سياسات توطين البيانات لأجل الحد من المراقبة الأجنبية على البيانات كأحد دوافعها، في حين تم استخدامها من قِبل البعض الآخر لأجل الرقابة الداخلية على البيانات والمعلومات المهمة لمواطنيها لاعتبارات سياسية.
٣. تمثل سياسات توطين البيانات نقطة إيجابية للحفاظ على الأمن القومي في ملف تأمين البيانات الحيوية، ومكافحة الإرهاب الداخلي، وإنفاذ القانون المحلي، وإنجاز بعض القضايا العالقة بسبب نقص الحصول على المعلومات.
٤. سياسات توطين البيانات ليست الضمانة الوحيدة لحماية البيانات ضد التهديدات السيبرانية، حيث تتعرض البيانات المخزنة في الداخل لمخاطر التهديد السيبراني بدرجة تفوق البيانات المخزنة في الخارج.

References.

*** أتوجه بالشكر والعرفان والامتنان لكل من؛ أ.م.د/ عبد الرحمن عبد العال، د/رضوى عمار، لجهديهما وإخلاصيهما في توجيهي وإرشادي لأجل إتمام تلك الدراسة.**

1. Encyclopedia, data localization, access date; 10.9.2021, available for; https://encyclopedia2.thefreedictionary.com/data+localization.
2. Data Localization accessed; 10.9.2021, 4:07pm, available for; https://www.drishtiias.com/printpdf/%20Data-Localisation.
3. Panday J, yoti, THE POLITICAL ECONOMY OF DATA LOCALIZATION, **The Open Journal of Sociopolitical Studies,** 2018, p521.
4. Ursic, Helena and others, **Handbook on Data Science and Law,** Chapter: Data localization measures and their impacts on data science, p3, available for; https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3102890_code2688716.pdf?abstractid=3102890&mirid=1.
5. Lindsey R. Sheppard, Erol Yayboke, Carolina G. Ramo, THE SHIFT TOWARD DATA LOCALIZATION, CSIS international security program, 2021.
6. Constantin urban, the cloud of a bloodless war; data localization and the securitization of cyberspace in India, **master's degree**, Vienna, 2021, pp17.

7. NIGEL CORY AND LUKE DASCOLI, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION, JULY 2021, pp6.
8. Swami Vivekananda, **DATA LOCALISATION IN A GLOBALISED WORLD DATA LOCALISATION IN A GLOBALISED WORLD An Indian Perspective an Indian Perspective**, The Dialogue C/O Foundation for Progressive Narrative, Published on 18th November 2018m pp 18.
9. NIGEL CORY AND LUKE DASCOLI, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, ibid, pp9
10. Jeremy Malcolm and Jyoti Panday, THE POLITICAL ECONOMY OF DATA LOCALIZATION**, Journal of Sociopolitical Studies,** Issue 11(2) 2018, pp 516.
11. Jayant Pankaj, CCTV Surveillance Is Rising in India, World, but Crime Rates Remain Unaffected, 2022, available at; https://bit.ly/3tlGjXL, accessed; 6.11.2022, 8:40pm.
12. Jason Burke, NSA spied on Indian embassy and UN mission, Edward Snowden files reveal, ibid.
13. Emily Wu, Sovereignty and Data Localization, ibid, pp17.
14. John Selby, Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both? ibid, pp16.
15. Limiting Location Data Exposure, National Security Agency, Cybersecurity Information, available at; https://media.defense.gov/2020/Aug/04/2002469874/-1/-1/0/CSI_LIMITING_LOCATION_DATA_EXPOSURE_FINAL.PDF.
16. Swami Vivekananda, DATA LOCALISATION IN A GLOBALISED WORLD DATA LOCALISATION IN A GLOBALISED WORLD An Indian Perspective, ibid, pp17.
17. Jonah Force Hill, THE GROWTH OF DATA LOCALIZATION POST-SNOWDEN: ANALYSIS AND RECOMMENDATIONS FOR U.S. POLICYMAKERS AND INDUSTRY LEADERS, **LAWFARE RESEARCH PAPER SERIES**, vol 2, no3, July 2014, pp27,28.
18. AWS Innovating Securely, does data localization cause more problems than it solves, pp5, available at; https://aws.amazon.com/compliance/data-privacy/?nc1=h_ls.
19. What Is Stuxnet? Musarubra US LLC, 2022, available at; https://www.trellix.com/en-us/security-awareness/ransomware/what-is-stuxnet.html, accessed; 14.8.2022, 9:22pm.
20. P. W. SINGER AND ALLAN FRIEDMAN, **CYBERSECURITY AND CYBERWAR WHAT EVERYONE NEEDS TO KNOW**, United States of America, Oxford University Press, 2014, Pp35,36.
21. Peter Swire and DeBrae Kennedy-Mayo, "The Effects of Data Localization on Cybersecurity", Draft – as of February 2022, pp6,7.
22. Nivedita Singh, Cyber Crimes in India Spiked Nearly Nine Times Since 2013, UP Topped Chart in 2020: Data, CNN-News18, New Delhi, September 2021, available at; https://bit.ly/3GSciqs, accessed; 27.11.2022.
23. Tanushree Basuroy, Number of cybercrimes reported across India from 2012 to 2021, Oct 13, 2022, available at; https://bit.ly/3Ue3E8q, accessed; 27.11.2022, 8:40 pm.
24. Emily Wu, Sovereignty and Data Localization, ibid, pp15.
25. Yanqing Hong, DATA LOCALISATION: DECONSTRUCTING MYTHS AND SUGGESTING A WORKABLE MODEL FOR THE FUTURE. THE CASES OF CHINA AND THE EU, BRUSSELS PRIVACY HUB WORKING PAPER VOL. 5 • N° 17 • AUGUST 2019, pp 8.
26. Jeremy Malcolm and Jyoti Panday, THE POLITICAL ECONOMY OF DATA LOCALIZATION, ibid, pp517.
27. Constantin urban, the cloud of a bloodless war; data localization and the securitization of cyberspace in India, ibid, pp23.

٢٨. إيهاب خليفة، National Internets لماذا تتوجه الدول نحو بناء شبكات اتصالات وطنية؟، مرجع سابق.

29. Internet shutdowns in 2021 report: digital authoritarianism returning across the globe, 2022, available at; https://bit.ly/3BGaygX, accessed; 14.9.2022, 7:16pm.
30. Charles Griffiths, The Latest 2023 Cyber Crime Statistics, February 2023, available at; https://aag-it.com/the-latest-cyber-crime-statistics/, accessed; 9.2.2023, 11:02 pm.
31. The use of the Internet for terrorist purposes, United Nations Counter-Terrorism Implementation Task Force, New York, 2012, pp3,4.

32. Napier, 11 of the biggest FinCrime and money laundering facts, 2022, available at; https://www.napier.ai/post/financial-crime-statistics-2022, accessed; 9.2.2023, 10:50pm.
33. . Rajat Kathuria and others, Economic Implications of Cross-Border Data Flows, 2019, pp 27.
34. john Selby, Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both? ibid, pp17.
35. Richard D. Taylor, "Data localization": The internet in the balance, ibid, pp6.
36. Claire Scharwatt, The impact of data localization requirements on the growth of mobile money-enabled remittances, GSMA Mobile Money, 2019, pp2.
37. SCOTT LIVINGSTON AND GRAHAM GREENLEAF, DATA LOCALISATION IN CHINA AND OTHER APEC JURISDICTIONS, 3 Privacy Laws & Business International Report, UNSW Sydney NSW 2052 Australia, October 2016, pp3.
38. Ibid.
39. Claire Scharwatt, The impact of data localization requirements on the growth of mobile money-enabled remittances, ibid, pp2.
40. Helena Ursic and others, Data Science and Law, Data localization measures and their impacts on data science, ibid, pp6.