توطين البيانات الشخصية في بعض الدول العربية / دراسة في ضوء أحكام القانون الدولي لحقوق الأنسان

أ.د. سامر محي عبد الحمزة
كلية القانون / جامعة واسط / العراق
smuhhi@uowasit.edu.iq
أ.م.د. أحمد تقي فضيل
كلية القانون / جامعة واسط / العراق
ahmedtaqi@uowasit.edu.iq

Localization of personal data in some Arab countries / a study considering the provisions of international human rights law

Prof. Samer Muhey Abdulhamza
College of Law\ Wasit University\ Iraq
Assit. prof. Ahmed Taqi Fadheel
College of Law\ Wasit University\ Iraq

المستخلص:

شهد العقد الأخير انتشاراً واسعاً لقوانين توطين البيانات الشخصية التي تشترط على الشركات الأجنبية العاملة في مجال الاتصالات وتكنولوجيا المعلومات مثل شركة غوغل (Google) وشركة أبل (Apple) على أن تقوم بمعالجة البيانات

الشخصية لمواطني الدولة ضمن حدود الدولة ذاتها وليس ضمن أي مكان خارج إقليم الدولة، وقد فتحت هذا القوانين الباب أمام النقاش حول مدى حق الدولة في توطين بيانات مواطنيها وأثر ذلك على حقوق الأنسان المحمية دولياً.

وفي بحثنا هذا سنسلط الضوء على فحوى هذا النقاش من ناحية تشريعات التوطين في بعض الدول العربية ومبرراتها، ومدى توافقها مع القانون الدولي وأثرها على الحقوق المحمية دولياً .

الكلمات المفتاحية: توطين البيانات، تأميم الاستثمارات الأجنبية، حقوق الأنسان المحمية دولياً.

Abstract:

The last decade has witnessed a wide spread of laws on the localization of personal data that require foreign companies working in the field of communications and information technology such as Google and Apple to process the personal data of the citizens of the country within the borders of the country itself and not anywhere outside the territory of the state, and these laws have opened the door to debate about

the extent of the state's right to localize the data of its citizens and its impact on the internationally protected human rights.

In this paper, we will shed light on the content of this discussion in terms of localization legislation in some Arab countries and their justifications, their compatibility with international law and their impact on internationally protected rights.

Keywords: data localization, nationalization of foreign investments, internationally protected human rights.

المقدمة

في ٦ شباط عام ٢٠٢٣ أعلنت شركة مايكروسوفت (Microsoft) عن نيتها بإنشاء مركز عملاق لمعالجة البيانات الرقمية في المملكة العربية السعودية ليتم فيه معالجة البيانات الخاصة بالأشخاص السعوديين داخل المملكة، وتمتد مهامه فضلا عن المملكة عموم دول الشرق الاوسط، وقد كان اهم اسباب هذا الإعلان هو الاستجابة لتعليمات حماية البيانات الشخصية الصادر بالأمر الملكي رقم (م/١٩) لسنة ٢٠١٩[١]، فالمملكة العربية السعودية هي احدى الدول التي اتجهت نحو قوانين التوطين لحماية البيانات الرقمية لمواطنيها، فالعقد الأخير شهد صدور مجموعة قوانين في الدول العربية موضوعها توطين البيانات منها قانون حماية خصوصية البيانات الشخصية القطري رقم (١٣) لسنة ٢٠١٦[٢]، وقانون حماية البيانات الشخصية الأردني رقم (٢٤) لسنة ٢٠٢٣[٣]، والقانون الاتحادي الإماراتي لحماية البيانات الشخصية الصادر بالمرسوم بقانون رقم (٤٥) لسنة ٢٠٢١،[٤] وقانون حماية البيانات الشخصية المصري رقم (١٥١) لسنة ٢٠٢٠[٥]، وقانون حماية البيانات الشخصية البحريني رقم (٣٠) لسنة ٢٠١٨[٦]، وجميعها تتضمن شكل من أشكال تقييد سلطة شركات التقانة في التعامل مع البيانات الخاصة برعايا الدولة، وفي العراق، فعلى الرغم من طرح الموضوع أمام مجلس النواب لكن المطالبات في تزايد لتشريع قانون لحماية البيانات الشخصية، فقد نقلت وكالة الأنباء العراقية عن مطالبة مركز الإعلام الرقمي لمجلس النواب بتشريع قانون لحماية البيانات الشخصية بسبب ما يشهده العراق من انتشار لبيع البيانات الشخصية والتعدي على منظومات شبكات التواصل الاجتماعي[٧].

هذه القوانين أثارت اهتمام الباحثين في القانون الدولي، فالبعض نظر اليها على أنها موجة جديدة من قوانين التأميم للشركات الأجنبية مشابهة لتلك الموجة التي سادت سبعينات القرن الماضي وان التوطين أصبح ينصب على البيانات لأنها أصبحت مشابهة للنفط من حيث القيمة الاقتصادية والتجارية. وهناك

من بحث الموضوع من ناحية مدى حق الدولة في توطين البيانات، في حين ركز قسم آخر من الباحثين على آثار هذه القوانين على الحقوق المحمية دولياً.

مشكلة البحث

مشكلة البحث تتركز في سؤال رئيس هو: هل تتوافق القوانين العربية في التوطين مع قواعد القانون الدولي؟ وما هو أثرها على حقوق الإنسان المحمية دولياً؟

منهج البحث

سنعتمد المنهج التحليلي منهجاً رئيساً مع الاستعانة بالمناهج الأخرى متى دعت الضرورة مثل المنهج المقارن.

خطة البحث

سوف نقسم هذا البحث على ثلاثة مباحث نتناول في المبحث الأول مفهوم توطين البيانات ومبرراته ثم نتناول في المبحث الثاني مدى حق الدولة في توطين البيانات وفي المبحث الثالث أثر توطين البيانات على الحقوق المحمية دولياً.

المبحث الأول

مفهوم توطين البيانات ومبرراته

التوطين هو سياسة تشريعية تنصب على البيانات وهذا يستدعي بيان مدلول البيانات ثم دراسة مفهوم التوطين، كما إن تشريعات التوطين ترتبط بعوامل كثيرة بعضها يتم الإعلان عنه في قوانين التوطين والآخر لا يتم الإعلان عنه لأسباب متعددة.

عليه سوف نقسم هذا المبحث على مطلبين نتناول في المطلب الأول تعريف توطين البيانات ونتناول في المطلب الثاني مبررات توطين البيانات.

المطلب الاول

تعريف توطين البيانات

لغرض تعريف توطين البيانات بوصفه سياسة تشريعية يجب ابتداء توضيح المقصود بالبيانات محل التوطين، فهذه الكلمة تحتاج بيان ما الذي يندرج ضمن هذا المفهوم وما الذي يخرج عنه، لذلك سوف نتناول تعريف البيانات في (الفرع الأول) ثم نتناول تعريف توطين البيانات في (الفرع الثاني).

الفرع الأول- تعريف البيانات

يتطلب تعريف البيانات أن نتناوله من جوانبه الثلاثة وهي اللغوية والتقنية والقانونية، لذا سوف نبحثه في الفقرتين الأتيتين:

أولاً. التعريف اللغوي

إن البحث في المدلول اللغوي للبيانات يبين أنها ترجمة لكلمة (Data)، وهي كلمة إنكليزية ذات أصول لاتينية يعرفها قاموس (Webster's) بانها "معلومات مخزونة بصيغة رقمية يمكن نقلها أو معالجتها إلكترونياً"[٨]. وتعرفها المعاجم العربية بانها "البيانات الخام التي يشتغل عليها الحاسوب وتتكون من تعبير رقمي وغير رقمي عن أحداث أو حقائق ماضية أو مقبلة بقصد تخزينها ومعالجتها للحصول على نتائج محددة"[٩].

ثانياً. التعريف التقني

إن البيانات بالمفهوم التقني لا يختلف كثيراً عن المفهوم اللغوي، إذ تشير الى تلك الحقائق أو المعلومات المخزنة بطريقة رقمية يمكن للحاسوب أن يتعامل معها.

لكن البيانات بهذه المفهوم تغطي مجموعة كبيرة من الأشياء والأفعال لا يمكن الإحاطة بها؛ لذلك فهي تحتاج الى تفصيل لبيان أي البيانات التي ستكون محلاً للحماية، لان كل نشاط يقوم به الفرد على الشبكة العنكبوتية يشكل بيانات سواء تعلق بمشاهدة فيديو أو ممارسة ألعاب ترفيهية أو كتابة تعليق على منشور في تطبيقات التواصل الاجتماعي، كما يشمل ذلك أيضاً البيانات التي تشير الى الشخص ذاته مثل اسمه عمره ومكان سكنه وعدد أفراد أسرته ومركزه المالي.

والاهتمام انصب مؤخراً على البيانات الشخصية للأفراد التي بقيت حتى نهايات القرن العشرين سرية لا يعرفها إلا هو وأجهزة الدولة التي كثيراً ما تحتفظ بها في دوائرها المختصة، فالدولة وحدها تحتكر المعلومات الرئيسة سواء كانت مالية مثل الضرائب والأملاك أو شخصية مثل مكان السكن أو أمنية مثل التوجهات السياسية، لكن مع ظهور الأنترنت والتحول الى الاقتصاد الرقمي أصبحت هذه المعلومات -وبالأخص المتعلقة بميول الشخص وأذواقه -متاحة للشركات التي تطلبها شرطاً للتسجيل في تطبيقاتها مثل شركة (Meta) مالكة تطبيق التواصل الاجتماعي الفيسبوك وتطبيق الإنستغرام.

ثالثاً. التعريف القانوني

إن إعطاء البيانات مفهوماً قانونياً لا يخلو من صعوبة وتعقيد لان تطويع هذه الكلمة لأغراض قوانين حماية البيانات بإضفاء حماية قانونية عليها يجب أن يرافقه تحديد وافٍ وشامل، فليس كل البيانات تستدعي الحماية، كما أن التعريف الذي سيقدمه المشرع لابد أن يتأثر بالغاية من التشريع، فتعريف البيانات لأغراض مكافحة الجريمة الإلكترونية سيكون أوسع من تعريفها لأغراض إجراء التعاملات الإلكترونية، لذلك نلاحظ أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠ مثلاً عمدت الى توسيع معنى البيانات لأغراض الملاحقة الجنائية فعرفت البيانات بانها "كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات كالأرقام والحروف والرموز وما اليها[١٠] .

أما قوانين حماية البيانات محل البحث فقد اهتمت بنوعين من البيانات التي ترى أنها الأجدر بالحماية وهي البيانات الشخصية والبيانات الشخصية الحساسة، فالبيانات الشخصية كما عرفها قانون حماية البيانات الشخصية الأردني رقم (٢٤) لسنة ٢٠٢٣ أنها "أي بيانات أو معلومات تتعلق بشخص طبيعي ومن شأنها التعريف به بطريقة مباشرة أو غير مباشرة مهما كان مصدرها أو شكلها بما في ذلك البيانات المتعلقة بشخصه أو وضعه العائلي أو أماكن تواجده".

ويعرف القانون ذاته البيانات الشخصية الحساسة بأنها "أي بيانات أو معلومات تتعلق بشخص طبيعي تدل بصورة مباشرة غير مباشرة على أصله أو عرقه أو تدل على آرائه او انتماءاته السياسية أو معتقداته الدينية أو أي بيانات تتعلق بوضعه المالي أو بحالته الصحية أو الجسدية أو العقلية أو الجينية أو بصماته الحيوية (البيومترية) أو بسجل السوابق الجنائية الخاص به".

وبذلك تصبح البيانات في المفهوم القانوني مقتصرة على البيانات ذات الطابع الشخصي من غير أن تشمل سائر البيانات الأخرى التي قد يتركها الشخص عن الدخول للأنترنت أو القيام بأعماله عن طريق الشبكة العنكبوتية.

الفرع الثاني- تعريف توطين البيانات

يقصد بتوطين البيانات ((Data localization مجموعة القوانين أو التعليمات تلزم الدولة بمقتضاه الشركات الكبرى العاملة في مجال تقنية المعلومات والتي تحصل على بيانات شخصية بحكم عملها مثل شركة غوغل (Google) وشركة مايكروسوفت (Microsoft)وشركة أمازون (Amazon) بأن تكون معالجة البيانات الخاصة بالمشتركين ضمن حدود الدولة نفسها وليس في الخوادم (السيرفرات) الموجودة في دول أخرى، كما تشمل أحياناً اشتراط الحصول على إذن الشخص عند معالجة بياناته وعدم تحويلها لشخص ثالث إلا بموافقة الجهات المختصة في الدولة[١١].

مع ملاحظة ان القوانين العربية لا تستخدم مصطلح التوطين، وإنما تستخدم مصطلح حماية البيانات، لكن التوطين هو الوصف الذي يستخدمه الباحثين في ميدان القانون الدولي -وهو الأقرب للواقع- لكون هذه القوانين تتطلب معالجة البيانات وطنياً داخل أراضي الدولة ولا تجيز معالجتها خارج الدولة، فهي عملية توطين.

والقوانين العربية صاغت فكرة التوطين عن طريق تقييد معالجة بيانات رعاياها، حتى لو تم من شركة يقع مركزها خارج الدولة طالما كانت البيانات لمواطنيها، فقد تبنت اغلب القوانين المعالجة الوطنية للبيانات الشخصية، فالقانون المصري مثلاً حظر أي عمليات نقل للبيانات الشخصية أو تخزينها أو مشاركتها التي تم جمعها للمعالجة الى دولة اجنبيه إلا بترخيص أو تصريح من مركز حماية البيانات الشخصية، لذلك فأي عملية حركة للبيانات الشخصية خارج النطاق الجغرافي لجمهورية مصر العربية

لا يجوز سواء تعلق الأمر بالتخزين أو الإتاحة أو التسجيل أو التداول أو النشر أو الاستخدام أو العرض أو الأرسال أو الاستقبال أو المعالجة."[١٢].

والأمر ذاته في قانون حماية البيانات الشخصية السعودي لعام ٢٠٢١ وقانون حماية البيانات الشخصية البحريني لعام ٢٠١٨.

وقد اشترطت هذه القوانين على الشركات الأجنبية أن تعين ممثلاً مفوضاً للشركة داخل الدولة لمباشرة التزاماته بموجب هذا القانون[١٣].

وينظر عدد من الباحثين الى أن الدولة حينما تقوم بالتوطين فهي تقوم بمد حماياتها لحق الشخص في سلامة بياناته لأنه حق من حقوق الأنسان متفرع من نظرية الحق الفردي بالتحكم بمعلوماته الشخصية، فالفرد هو المالك لهذه المعلومات، وهذا يتفرع عنه حقه في الأذن أو عدم الأذن باستخدام هذه المعلومات وحقه في معرفة الى أي مدى يتم إذاعة معلوماته ولأي غرض ولأي جهة [١٤].

والتوطين بوصفه سياسة تشريعية ظهر ابتداءً بسبب التجاوز على البيانات من قبل شركات التقانة الكبرى، فقد خلقت الحوادث الخاصة بالتجسس والاستخدام غير المشروع جواً من عدم الثقة بين شركات التقانة الكبرى وبين الدول، إذ بينت تلك الحوادث إن تلك الشركات تستغل بيانات المشتركين لعدة أغراض منها:

أ. أغراض تجارية: مثل معرفة السلع التي يفضلها ومعرفة السلوك الاستهلاكي، فقد تم إدانة شركة ميتا (Meta) المالكة للفيسبوك والإنستغرام في مرات عديدة بالاستخدام غير المشروع للبيانات لأغراض تجارية كان آخرها إدانتها من قبل الاتحاد الأوروبي عام ٢٠٢٢ ولاستخدامها البيانات لمحاولتها كسر قوانين التنافس التجاري[١٥].

ب. أغراض سياسية: مثل استخدام البيانات لمعرفة الاتجاه السياسي للفرد لإرسال أخبار أو إعلانات أو وسائط من شانها التأثير على موقفه السياسي واختياراته الانتخابية، وقد أدينت شركة ميتا (Meta) أيضاً استخدام البيانات لأغراض الدعاية السياسية أوائل عام ٢٠١٨ ذاتها وإلزامها بدفع مبلغ (٧٢٥) مليون دولار بسبب تسريع بيانات (٨٧) مليون مستخدم الى شركة استغلتها في الدعاية السياسية واستخدمتها حملة الرئيس الأمريكي السابق دونالد ترامب [١٦].

ت. أغراض أمنية: ولعل هذا أخطر ميدان لاستغلال البيانات لأنه يرتبط بأمن الدولة، ويتمثل بالتجسس وجمع البينات الخاصة بالدول الأخرى بما فيها جمع الأسرار العسكرية والمحادثات السرية. إذ كشفت التسريبات التي أذاعها المتعاقد في وكالة الأمن القومي الأمريكي إدوارد

سنودن عام ٢٠١٣ عن تعاون شركات التقانة مع الجهات الأمنية الأمريكية في مراقبة البيانات الشخصية والاطلاع عليها، وقد تم فرض غرامة تجاوزت المليار دولار لإتاحة بيانات المستخدمين لأجهزة الامن الأمريكية[١٧].

المطلب الثاني- مبررات التوطين

أوردت قوانين حماية البيانات العربية أسباباً لتشريعها تتمحور حول حماية البيانات وتطبيق القانون، مع ذلك هناك الكثير من الأسباب التي لا تفصح عنها الدول بعضها ذات طبيعة اقتصادية وأخرى ذات طبيعة سياسية.

لذا سنتناول في هذا المطلب المبررات المعلنة في الفرع الأول والمبررات غير المعلنة في الفرع الثاني.

الفرع الأول

المبررات المعلنة

إن التشريعات العربية تدرج حماية البيانات الشخصية سبباً رئيساً لتشريعها، وهي بهذا تساير النظام الأوروبي العام لحماية البيانات لعام ٢٠١٦ الذي جعل الهدف الأساس من تشريعه هو حماية الأشخاص الطبيعيين فيما يتعلق معالجة بياناتهم الشخصية وحماية الحقوق والحريات الأساسية للأفراد واهمها الحق في حماية بياناتهم الشخصية[١٨].

فقد منحت القوانين العربية الفرد مجموعة من حقوق أهمها:

اولا- حق الاطلاع

وتشمل عدد من الصلاحيات يمكن اختصارها بانها حق الشخص بمعرفة البيانات التي يجري معالجتها، وهو حق كما يصفه القانون الأردني بأنه حق في (العلم والاطلاع والوصول) ويشمل ذلك الحق في العلم والمعرفة باي خرق أو انتهاك أو إخلال بأمن وسلامة بياناته[١٩].

ثانيا. الحق في التعديل

ويشمل ذلك مجموعة أكبر من الصلاحيات تتعلق بحقه بتعديل بياناته أو الإضافة اليها أو تحديثها، أو نقلها أو تخصيص المعالجة، كما إن له حق سحب الموافقة السابقة، بل ذهبت القوانين الى ابعد من ذلك بان أجازت له محو بياناته أو إخفائها كلياً[٢٠].

ثالثا. الحق في الاعتراض

ويشمل ذلك حقه في الاعتراض ضد الجهات التي تتولى معالجة بياناته إذا اعتقد أن المعالجة كانت غير ضرورية لتحقيق الأغراض التي جمعت البيانات من أحلها.

وعلى الرغم من أن كثيراً من القوانين العربية لم تبين آلية الاعتراض أو مكانه أو إجراءاته، إلا أن بعضها كالقانون البحريني فصل ذلك بأن حدد آليات الاعتراض والتزامات مدير البيانات مع وضع حد زمني لإجراءات الاستجابة لاعتراض الفرد، وقد شمل الاعتراض حالات كثيرة منها الاعتراض على المعالجة التي تتم لأغراض التسويق المباشر وفي حالة رفض اعتراضه يجوز الطعن أمام هيئة عليا، كذلك الاعتراض على المعالجة التي تلحق ضرراً مادياً أو معنوياً بصاحب البيانات والاعتراض على المعالجة التي تتم بناء عن المعالجة الآلية [٢١].

الفرع الثاني

المبررات غير المعلنة

تؤدي الظروف السياسية والاجتماعية دوراً في توجيه القوانين، واحياناً لا يفصح المشرعون الأسباب الحقيقية لتشريعها، أو لا يدرجونها ضمن الأسباب الموجبة للتشريع، وقوانين التوطين لا تشير أكثر من ذكر (حماية البيانات الشخصية) سبباً للتشريع، لكن بعض الباحثين يرى أن الأسباب الحقيقة هي دوافع أخرى، وبالأخص مبررات اقتصادية وأمنية، وهو ما سنتناوله في الفقرتين الأتيتين.

أولاَ. المبررات الاقتصادية

في ظل الاقتصاد الرقمي سريع التطور أصبحت البيانات عصب هذا الاقتصاد، لقد باتت البيانات الرقمية كما وصفها الرياضي البريطاني كلايف همبي هي النفط الجديد [٢٢].

وقد لاحظت العديد من الدول إن الشركات العملاقة تستخدم تلك البيانات لمعرفة سلوك المستهلك والترويج لبضائعها من غير أن تهتم ببناء بنى تحتية أو استثمار حقيقي في الدولة التي تستخدم بيانات مواطنيها، مما أدى الى إضعاف الشركات الوطنية لافتقارها لتلك البيانات المهمة، لذلك تحاول الدول إلزام تلك الشركات بمشاركة تلك البيانات مع الشركات الوطنية [٢٣].

وقد مثلت القوانين في إفريقيا والهند انعكاساً لهذا الاتجاه، فقد عانت هذه الدول في الماضي من الاستعمار الذي كان سبباً في تأخر تلك الدول، وهناك قناعة لدى هذه الدول أن ما تقوم به الشركات هو استعمار رقمي لا يختلف كثيراً عن الاستعمار التقليدي بمفهومه القائم على تعظيم الأرباح باقل خسارة، فالاستعمار الرقمي هو "عملية السيطرة على البيانات واستغلالها من الأفراد برضاهم أو بدون موافقة صريحة عن طريق شبكات الاتصال التي تملكها شركات التقانة الغربية"[٢٤] فهذه الشركات لا تترك مجال للمنافسة من قبل الشركات الوطنية وتحتكر بيع الخدمات الإلكترونية وإيجارها بشكل برمجيات وتضع برامج تعقب تتيح لها معرفة التفاصيل الكاملة للأفراد مما يسهل عليها معرفة رغبات المستهلكين وبالتالي عرض البضاعة الملائمة لتلك الرغبة[٢٥].

والاتحاد الأوروبي هو الآخر بدء ينظر لعملية التوطين بوصفها هدف لتشريعات الاتحاد والغرض الأساس هو حماية الصناعة الأوروبية من السيطرة الكاملة للشركات الأمريكية على السوق الرقمية الأوروبية، وفعلاً أصدر الاتحاد الأوروبي ما عرف باسم (النظام الأوروبي لحماية البيانات لعام ٢٠١٦) الذي منع معالجة البيانات الشخصية لمواطنيه خارج الاتحاد الأوروبي.

ثانياً. المبررات الأمنية

إن بعض المنظمات الدولية غير الحكومية المعنية بحقوق الأنسان مثل منظمة هيومن رايت ووتش (Human Rights Watch) بينت في تقاريرها إن حماية أمن المعلومات للأفراد قد يراد منه في الحقيقة حماية نظام الحكم وإبعاده من أي انتقاد.

فالفلسفة الاشتراكية في الحكم التي حافظت على وجودها في كل من الاتحاد الروسي والصين التي تضفي على الدولة ومؤسساتها وقادتها نوعاً من القدسية تمنع مطلقا أي انتقاد لها وتعرض المنتقد الى ملاحقة أمنية، بل إن المطالبة بالحقوق الفردية هي فكرة مرفوضة تماماً لأنها تحمي الملكية الخاصة ومن ثم تساهم في استغلال الطبقة العاملة"[٢٦].

فقد لاحظت بعض المنظمات المعنية بحرية الرأي على الأنترنت أن العامل الأمني هو المحرك الأساس لقوانين حماية البيانات في الدول ذات النظم الشمولية وذات الحزب الواحد كالصين وروسيا وكوريا الشمالية وعدد من الدول العربية مثل المملكة العربية السعودية ومصر، فالهدف الأساس من هذه التشريعات هو تعقب نشاط المعارضين للنظام والذين يدلون بتعليقات تتضمن انتقاداً للدولة، فهذه الدول لا تتسامح مع انتقاد الفئة الحاكمة أو سياساتها والانتقاد في بعض الدول يشكل جريمة مثل المساس بشخص القائد أو الرئيس أو الملك.

ويفسر ذلك تسابق الدول المعروفة بانتهاكات حقوق الإنسان الى إقرار قوانين حماية البيانات الشخصية لأنها تمكن تعقب كل تعليق أو نشاط في الفضاء السيبراني للأفراد لذلك تستخدمها المنظومة الأمنية لملاحقة هؤلاء، لذلك فقد عارضت (١٨) منظمة حقوقية قيام شركة مايكروسوفت بأنشاء مراكز تخزين للبيانات في المملكة العربية السعودية لأنها ترى أن نظام حماية البيانات السعودي الجديد ولوائحه التنفيذية تمنح الهيئات الحكومية سلطات واسعة في الوصول الى البيانات الشخصية للأفراد لذلك ستجبر تلك السلطات شركة مايكروسوفت على تسليم البيانات الشخصية في مراكز التخزين العائدة لها لغرض ملاحقتهم امنياً[٢٧].

وفي مصر نقلت الصحافة عن انتقاد عدد من المعنيين بحقوق الأنسان لقانون حماية البيانات الشخصية المصري، إذ أن إقرار هذا القانون كان سببه دافعاً امنياً لتمكين جهات الأمن القومي من الحصول على بيانات المواطنين وتقنين حرية الاطلاع عليها في ظل غياب أي رقابة قضائية على ذلك، وحتى عند

مناقشة القانون واجه اعتراضاً من بعض النواب الذين رأوا فيه قانون مقيد للحرية وبعيد عن الواقعية التي تعالج بها قوانين البيانات الشخصية [٢٨].

المبحث الثاني

حق الدولة في توطين البيانات

إن الحق في توطين المعلومات في القانون الدولي العام يرتبط بموضوع تأميم الاستثمارات الأجنبية وحدوده، لذلك سوف نقسم هذا المبحث على مطلبين نتناول في المطلب الأول مدى حق الدولة في توطين البيانات ونتناول في المطلب الثاني قيود توطين البيانات.

المطلب الأول- مدى حق الدولة في توطين البيانات

إن البيانات الرقمية قد تم نقلها الى شركات التقانة الكبرى بموجب اتفاقية ترخيص تعطي الشركة صلاحيات واسعة في التعامل معها، فهل للدولة التي يتمتع الأشخاص بجنسيتها حق في استعادة هذه البيانات أو تقييد حق الشركة في التصرف بها؟

الواقع إن الإجابة تستدعي النظر في القواعد الدولية التي تحكم حق الدولة في التعامل مع الاستثمارات الأجنبية في الدولة، وهي مسالة تم التصدي لها مبكراً من قبل محكمة العدل الدولية الدائمة في قضية مصنع شورزو عام ١٩٢٧، إذ قررت المحكمة وجوب التمييز بين وجود معاهدة دولية تمنع مصادرة الأصول الأجنبية من عدمه، ففي حالة وجود معاهدة تمنع ذلك فتتحمل الدولة المسؤولية الدولية اذا خالفت أحكام المعاهدة، أما في حالة عدم وجود معاهدة دولية فالأصل جواز ذلك مع التعويض، لذلك قررت المحكمة إن بولندا التي قامت بمصادرة الأصول المالية للرعايا الألمان في مصنع شورزو بالمخالفة للمادة (٩٢) من معاهدات فرساي لعام ١٩١٩ -التي تمنع مصادرة أموال الرعايا الألمان دون تعويض- خالفت التزاماتها الدولية لذلك يجب عليها تعويض الرعايا الألمان عن أعمال المصادرة[٢٩].

وقد أعادت محكمة العدل الدولية هذا المبدأ قي قضية شركة النفط الإنكليزية الإيرانية عام ١٩٥١ الذي قررت فيه أن التأميم حق لكل دولة ذات سيادة ولا يتدخل القانون الدولي إلا من حيث كون التأميم تم بمقابل تعويض عادل وسريع يكون فيه القضاء الداخلي المرجع الأساس [٣٠].

فللدولة مطلق الحرية في فرض التزامات على الشركات الأجنبية العاملة فيها سواء كانت وطنية أم أجنبية، لكن في حدود معينة، فحماية البيانات لا يجب أن يصل حد مصادرة لان مصادرة أموال الأجانب بشكل تعسفي ومن ثم يستتبع مسؤولية الدولة وفقاً للقانون الدولي، كما أن وجود هذه الشركات خارج حدود الدولة يواجه عدد من العقبات في سبيل إخضاعها للقوانين الوطنية.

المطلب الثاني- قيود التوطين

إن حق الدولة في الاستحواذ على الاستثمارات الأجنبية مقيد بمجموعة قيود وفقاً لقواعد القانون الدولي، هذه القيود تشمل:

١. أن يكون تصرف الدولة لأجل تحقيق المصلحة العامة.
٢. ألا يشتمل تصرف الدولة على تمييز بين الأجنبي والوطني.
٣. احترام القانون الدولي والمعاملة العادلة عند التعامل مع الاستثمارات الأجنبية.
٤. أن يكون مقابل تعويض عادل وسريع.
٥. أن يكون للشركة الحق في الاعتراض أمام القضاء [٣١].

ولكن هل من الممكن قياس عملية توطين البيانات على مصادرة أصول الشركات الأجنبية لكي نستطيع القول بتقيد الدول بالشروط السابقة عن إصدارها قرارات التوطين؟

في البدء يمكن القول إن قوانين التوطين التي تتضمن شروطاً بمنع معالجة البيانات خارج الدولة سيفرض أعباء مالية كبيرة على الشركات الأجنبية قد لا تستطيع تنفيذها بمفردها، فالتوطين يعني إما شراء خوادم جديدة يتم خزن المعلومات العائدة لرعايا الدولة فيها، أو بنقل بعض الخوادم من دول أخرى، وفي كلا الحالتين ستكون مكلفة على الشركة قد تدفعها الى إنهاء عملها في الدولة.

فهل يجب على الدولة أن تشارك في النفقات التي تتحملها الشركات في سبيل الإيفاء بمتطلبات حماية البيانات؟ وهل يمكن تطبيق شرط التعويض الذي تبنته محكمة العدل الدولية بخصوص تأميم حصص شركات النفط؟

في الوقت الحالي لا يمكن الإجابة بشكل قطعي لقلة التطبيقات وتباين مواقف الشركات والدول من الموضوع، مثلا حين أصدرت الصين قوانين التوطين وحاولت تطبيقها على شركة غوغل التي بدأت نشاطها في الصين ٢٠٠٦، بينت الشركة إنها لا تستطع الإيفاء بمتطلبات القوانين الصينية لذلك عمدت الى الغاء أعمالها في الصين والمغادرة عام ٢٠١٠ على الرغم من الخسائر التي تكبدتها [٣٢].

ووفقا للتقديرات المتوفرة فان تكلفة مغادرة الشركة للسوق الصينية تجاوزت مبلغ ٦٠٠ مليون دولار [٣٣].

وتكرر الأمر مع حلول مختلفة في علاقة المملكة العربية السعودية مع شركة مايكروسوفت، فبعد ان دخلت قوانين حماية البيانات حيز التنفيذ عام ٢٠٢٣ وألزمت الشركات أن يتم معالجة البيانات للمواطنين السعوديين داخل السعودية، أعلنت شركة مايكروسوفت أنها ستقوم بإنشاء خوادم ضخمة في المملكة تحتوي على مراكز بيانات للتوافق مع القوانين الجديدة، من غير الإشارة الى من الذي سيتحمل تكلفة المشروع وهل ستساهم المملكة في قسط من التكاليف [٣٤].

المبحث الثالث

أثر حماية البيانات على حقوق الإنسان المحمية دولياً

إن قوانين حماية البيانات بالمفهوم الذي بيناه قد يمثل تهديدا لحقوق الإنسان التي ضمنتها المواثيق الدولية ضمن ما يعرف بالقانون الدولي لحقوق الإنسان، فهذا الفرع الفتي للقانون الدولي العام يختص بكل ما يتعلق في دراسة الحقوق المحمية دوليا مثل الحق في التعبير والحق في حرية المعتقد والحق في المشاركة في الحياة السياسية.

وسوف نتناول تأثير حماية البيانات على هذه الحقوق في ثلاثة مطالب نتناول في المطلب الأول تأثير التوطين على الحق في حرية التعبير ونتناول في المطلب الثاني تأثير التوطين على الحق في الوصول الى المعلومة ثم نتناول في المطلب الثالث تأثير التوطين على الحق في محاكمة عادلة.

الفرع الأول- تأثير توطين البيانات على الحق في حرية التعبير

كفل العهد الدولي للحقوق المدنية والسياسية لعام ١٩٦٦ للأفراد حرية التعبير، إذ تضمن ما يأتي "لكل إنسان حق في حرية التعبير. ويشمل هذا الحق حريته في التماس مختلف ضروب المعلومات والأفكار وتلقيها ونقلها إلى آخرين دونما اعتبار للحدود، سواء على شكل مكتوب أو مطبوع أو في قالب فني أو بأية وسيلة أخرى يختارها."[٣٥].

وقد أجاز العهد تقييد هذا الحق لدواعٍ منها حماية النظام العام والآداب العامة، إلا أن المنظمات غير الحكومية المعنية بحقوق الإنسان لاحظت أن قوانين التوطين قد ترتبط مباشرة بمحاربة حرية الراي، إذ تمكن هذه القوانين الدولة من الاحتفاظ بقاعدة ضخمة من المعلومات عن أفراد المجتمع وآرائهم المكتوبة ثم استخدامها لمحاكمة المعارضين تحت تسميات غامضة مثل حماية قيم المجتمع أو حماية النظام العام أو نشر المعلومات المضللة في مصر أو حماية الأمن الوطني أو تمجيد الإرهاب[٣٦].

فمنظمة العفو الدولية أوردت في تقريرها السنوي عن حالة حقوق الإنسان في الدول العربية إن بعض هذه الدول تستخدم الملاحقة القضائية والأمنية ضد المعارضين والمنتقدين، ففي الجمهورية العربية السورية مثلا يشكل انتقاد السلطات الحاكمة جريمة تصل عقوبتها الى السجن لمدد طويلة، وقد نقلت الصحافة عن وزير الداخلية السوري عن القبض على احدى عشر مواطناً بتهمة نشر أخبار على موقع الفيسبوك[٣٧].

وفي جمهورية مصر العربية يتم اعتقال المعارضين بسبب نشاطهم على وسائل التواصل الاجتماعي، فقد تم اعتقال عدد من الناشطين ومنهم عبد السلام عبد الغني بعد أن أيد دعوات الاحتجاج في مؤتمر المناخ العالمي في القاهرة وكانت التهمة الموجهة اليه هي نشر أخبار كاذبة[٣٨].

وفي دولة الأمارات العربية المتحدة هناك ستة وعشرون سجيناً تم أدانتهم بسبب انتقادهم السياسي، لان القوانين الإماراتية تجرم نشر أخباراً من شانها الإساءة لسمعة الدولة أو هيبتها أو قادتها المؤسسين تصل عقوبتها الى ثلاث سنوات [٣٩].

ولعل أبرز حالة استرعت الاهتمام الدولي في استخدام قوانين حماية البيانات لملاحقة المعارضين هي في قطر حالة الناشط الكيني مالكوم بيدالي (Malcolm Bidal) الذي يعمل حارس امن في قطر الذي قام في نيسان عام ٢٠٢١ بأنشاء موقع باسم وهمي على تطبيق تويتر أرسل عن طريقه تقرير الى منظمة هيومن رايت ووتش عن حالة العمال الأجانب في قطر وسوء المعاملة التي يتعرضون لها، وبفضل قوانين حماية البيانات استطاعت السلطات القطرية معرفة هويته وتم إحالته الى المحاكمة بتهمة ارتباطه بقوى أجنبية لزعزعة استقرار البلد [٤٠].

الفرع الثاني- تأثير توطين البيانات على الحق في الوصول للمعلومة

تضمن العهد الدولي للحقوق المدنية والسياسية الحق في ويشمل هذا الحق حريته في التماس مختلف ضروب المعلومات والأفكار وتلقيها ونقلها إلى آخرين.

إلا أن قوانين التوطين تمنح السلطات الحكومية والأمنية صلاحيات واسعة في حجب المواقع الإلكترونية التي تعتقد أنها لا تتلاءم مع النظام السياسي القائم، ولعل من أكثر ما يهدد حق المواطن في تلقي المعلومة هو أن المؤسسات الإعلامية والصحف الإلكترونية على علم بان التوطين وتخزين المعلومات داخل الدولة سيمكن أجهزة الدولة من حجب أي موقع صحفي أو أخباري تعتقد فيه الدولة انه يتعارض مع سياستها، حتى لو كان ذا طبيعة ثقافية أو سياسية أو اجتماعية [٤١].

ففي الصين وروسيا وإيران مكنت قوانين التوطين هذه الدول من حجب عشرات الألاف من المواقع الإلكترونية التي ترى انه يتضمن انتقاداً أو تقريراً يتضمن جوانب سلبية ضد الحكومة، فمثلا في الجمهورية الإسلامية الإيرانية ولغاية ٢٠٠٨ حجبت الحكومة أكثر من خمسة ملايين موقع إلكتروني [٤٢].

الفرع الثالث- تأثير توطين البيانات على الحق في المحاكمة العادلة

أحاط العهد الدولي للحقوق المدنية والسياسية لعام ١٩٦٦ حقوق المتهم بمجموعة ضمانات تحميه من التعسف والظلم الذي قد يقع عليه من الأجهزة الأمنية، لذلك نص العهد على " الناس جميعا سواء أمام القضاء. ومن حق كل فرد، لدى الفصل في أية تهمة جزائية توجه إليه أو في حقوقه والتزاماته في أية دعوى مدنية، أن تكون قضيته محل نظر منصف وعلني من قبل محكمة مختصة مستقلة حيادية، منشأة بحكم القانون."[٤٣].

إن قوانين التوطين لا تتضمن أي رقابة قضائية، فالقانون المصري والسعودي والأردني لا يرسم آلية للطعن بالدليل المستخرج من البيانات الشخصية من الجهات الأمنية، بل يعطي للسلطة التنفيذية الحق في الاطلاع على البيانات دون إشعار طالما تعلقت بالأمن القومي والمصلحة العامة، وهذه التعبيرات شديدة العمومية ويمكن تفسيرها لتشمل حالات لا حصر لها لمراقبة البيانات الشخصية للأفراد.

لذلك نلاحظ أن احدى الانتقادات المهمة لقوانين حماية البيانات هي أنها منحت صلاحيات واسعة للأجهزة الأمنية ولم تعط ضمانات كافية للمواطن من خلال منح القضاء دور في مراقبة أعمال الحكومة الخاصة بالبيانات الشخصية، لذلك اقترح بعض الباحثين ضرورة أنشاء هيئة مستقلة تتولى الأشراف على إجراءات الدخول للبيانات الشخصية للأفراد (٤٤).

كما أن تشكيل مراكز إدارة البيانات في القانون المصري والأردني لا توحي باي ضمانات للشخص في مواجهة هذه الهيئات، فهذه الهيئات لا تتكون من أعضاء مستقلين، وإنما مرتبطين بهيئات الدولة؛ إذ يتم تعيينهم من الوزير وتتضمن الهيئة ممثلين عن الدفاع والأمن والاستخبارات على الرغم من أنها مؤسسة لها صلاحيات كبيرة في إصدار الأنظمة والتعليمات. (٤٥).

الخاتمة

في الختام توصلنا الى عدد من النتائج وقدمنا عدد من المقترحات هي ثمرة ما سبق من تحري فقرات البحث، وهي كالآتي:

أولاً. الاستنتاجات

١. ان الاهتمام بحماية البيانات الشخصية لم يظهر الا في العقد الاخير بعد الخروقات التي سادت نتيجة اهتمام الشركات الكبرى في مجال البيانات بتعظيم الأرباح من غير ان يقابل ذلك اهتمام بحماية تلك البيانات كان من نتيجته فقدان الثقة بأمانه تلك الشركات ومصداقيتها.

٢. حاولت الدول العربية ان تضع تشريعات تستهدف حماية البيانات عن طريق توطينها وعدم السماح لشركات التقانة الكبرى معالجة البيانات الشخصية خارج حدود الدولة الا في حالات استثنائية، الا ان تلك القوانين لم تمنح الافراد الضمانات الكافية لحماية بياناتهم. بل جعلتها مباحة للأجهزة الأمنية والاستخبارية واجازت استباحتها بدعوى حماية الامن الوطني.

٣. لم نجد قواعد دولية صريحة تحكم توطين البيانات مما جعل الأساس فيها هو الرجوع للمبادئ العامة في القانون الدولي وهي حق الدولة في التعامل مع الاستثمارات الاجنبية استناداً الى مبدا السيادة الاقليمية الذي يمتد ليشمل الفضاء السيبراني.

٤. لا تتفق القوانين العربية في بعض فقراتها مع المواثيق الدولية لحماية حقوق الانسان وبالذات العهد الدولي للحقوق المدنية والسياسية للعام ١٩٦٦، فالكثير من الحقوق المحمية دوليا جرى

تجاوزها ليس فقط على مستوى النصوص القانونية التي تفتقر من الحماية الحقيقة لها، وانما كذلك من ناحية تطبيق تلك التشريعات.

ثانياً. الاقتراحات

١. نرى ضرورة ان تسعى الدول العربية لاعتماد المعايير العالمية في حماية البيانات الشخصية مثل النظام الأوروبي لحماية البيانات لعام ٢٠١٦، وهذا ما سيساهم في توحيد معايير حماية البيانات الشخصية بين الدول العربية جميعها مما يمنح تلك القوانين الانسجام والتوافق.

٢. ضرورة اشراك جامعة الدول العربية في جهود اقرار معاهدة دولية عربية لحماية البيانات الشخصية، فقد سبق للجامعة ان نجحت في تبني اتفاقيات تتعلق بالتعاملات التجارية الالكترونية ومكافحة الجرائم الالكترونية فضلا عن اصدار معايير الامن السيبراني، لذلك لن يكون عملها في مجال حماية البيانات الشخصية مهمة عسيرة.

٣. على الدول العربية ان تتبنى موقفاً واضحاً من حقوق الانسان من خلال محاولة الالتزام بالمعايير العالمية التي اقرتها الامم المتمدنة والتي ستمنح الدول العربية فرصة جلب الاستثمارات الاجنبية وتحقيق خطط التنمية المستدامة التي هي في اشد الحاجة اليها، أما إطلاق يد الأجهزة في التجسس وملاحقة اصحاب الراي المعارض فسوف نكون أمام ربيع عربي جديد يطيح بالحكومات المستبدة وقوانينها.

الهوامش

(١) المنشور في الجريدة الرسمية عدد (م-١٩) في ١٤٤٣/٢/٩ هجرية.
(٢) المنشور في الجريدة الرسمية عدد (١٥) في عام ٢٠١٨.
(٣) المنشور في الجريدة الرسمية عدد (٥٨٨١) الصادر بتاريخ ٢٠٢٣/٩/١٧.
(٤) المنشور في الجريدة الرسمية عدد العدد (٧١٢) ملحق ١ في ٢٦ سبتمبر ٢٠٢١.
(٥) عدد (٢٨) مكرر في ١٥ يوليه سنة ٢٠٢٠.
(٦) المنشور في الجريدة الرسمية عدد (٣٣٥٧) في ١٩ يوليو ٢٠١٨.
(٧) الخبر منشور على الموقع الإلكتروني لوكالة الأنباء العراقية في ٢٠٢٣/١١/١٨ وعلى الرابط:
https://ina.iq/142478--.html/
(٩) المعجم الموحد لمصطلحات تقانة (تكنولوجيا المعلومات)، أشراف ا.د ميلود حبيبي، المنظمة العربية للتربية والثقافة والعلوم/ مكتب تنسيق التعريب، الدار البيضاء، ٢٠١١، ص٣٢.
(١٠) الفقرة (٣) من المادة الثانية من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠ والتي صادق عليها العراق بموجب قانون رقم (٣١) لسنة ٢٠١٣ والمنشور في الوقائع العراقية عدد (٤٢٩٢) في ٣٠ أيلول عام ٢٠١٣.
(11) Jennifer Daskal and Justin Sherman, Data Nationalism on the Rise, The Global push for state control of data, June 2020, p.3.
(١٢) المادة(١) والمادة (١٤) من قانون حماية البيانات الشخصية المصري.
(١٣) الفقرة (٣) المادة الثانية من قانون حماية البيانات الشخصية البحريني والفقرة م (٢) من المادة الثالثة والثلاثون من قانون حماية البيانات الشخصية السعودي.
(14) Yanqing Hong, Data Localization: Deconstructing myths and suggesting a workable model for the future. The cases of China and the EU, Working paper, Vol. 5 • N° 17 • August 2019, p.9.
(١٥) ينظر الخبر على الموقع الإلكتروني الرسمي لقناة العربية الإخبارية في ١٢مارس ٢٠٢٢ على الرابط
https://www.alarabiya.net/aswaq/companies/2022/03/12/
(١٦) ينظر الخبر على الموقع الإلكتروني الرسمي لقناة الجزيرة الإخبارية ٢١ مارس ٢٠١٨ على الرابط
https://www.aljazeera.net/encyclopedia/2018/3/21/
(١٧) ينظر الخبر على الموقع صحيفة القدس العربي الالكترونية في ٢٢ مايو ٢٠٢٢ على الرابط
https://www.alquds.co.uk /
(18) General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the council, 27 April 2016, Article 1 Chapter 1.
(١٩) الفقرة(ب) المادة (٤) من قانون حماية البيانات الشخصية الأردني رقم (٢٤) لسنة ٢٠٢٣.
(٢٠) المادة الرابعة من لتعليمات حماية البيانات الشخصية السعودي لعام ٢٠١٩.
(٢١) المواد (١٩-٢٢) من قانون حماية البيانات الشخصية البحريني رقم (٣٠) لسنة ٢٠١٨.
(22) Marcin Szczepański, Is data the new oil? Competition issues in the digital economy, European Parliamentary Research Service, January 2020, p.
(23) 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, p.6.
(24) Danielle Coleman, Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws, Michigan Journal of Race & Law, VOL. 24, 417, 2019, pp.422.
(25) Ibid., p.424.
(٢٦) لين هانت، نشأة حقوق الإنسان، لمحة تاريخية، دار كلمات عربية للترجمة والنشر، ٢٠١٣، ص١٨٨.
(٢٧) هيومن رايت ووتش، السعودية على مايكروسوفت تعليق خطط إنشاء مركز للبيانات، تقرير منشور على موقع المنظمة في ٢٣ أيار ٢٠٢٣.
(٢٨) محمد عبد الله، قانون "حماية البيانات الشخصية" بمصر.. ما علاقته بعقل الدولة تحت الأرض، موقع الجزيرة الإخباري، في ٢٠٢٠/٧/٢٤

([29]) Factory At Chorzów, Germany v Poland, Judgment, Claim for Indemnity, Merits, Judgment No 13, (1928) PCIJ Series A No 17, ICGJ 255 (PCIJ 1928), 13th September 1928.

([٣٠]) د. عصام العطية، القانون الدولي العام، بغداد، ١٩٩٢، ص٣٧٩.

([31]) Schrijver N. Sovereignty over Natural Resources: Balancing Rights and Duties. Cambridge University Press; 1997, p.344-352.

([٣٢]) Sunk wook kim and Aziz Douai, Google vs. China's "Great Firewall": Ethical implications for free speech and Sovereignty, Technology in Society · May 2012, p.175.

([33]) Rekha Dahiya, google is exit from china, A case study, Delhi Business Review X Vol. 11, No. 2 (July – December 2010), p.118.

([34])https://azure.microsoft.com/en-us/updates/in-development-new-planned-datacenter-region-in-saudi-arabia-saudi-arabia-central/

([٣٥]) الفقرة (٢) من المادة (١٩) من العهد الدولي للحقوق المدنية والسياسية لعام ١٩٦٦.

([36]) Adrian Shahbaz, Allie Funk and Andrea Hackl, User Privacy or Cyber Sovereignty? Assessing the human rights implications of data localization, Freedom House special report 2020, p.5.

([٣٧]) تقرير منظمة العفو الدولية للعام ٢٠٢٢/٢٠٢٣ حالة حقوق الإنسان في العالم، منشورات منظمة العفو الدولية، الطبعة الأولى، ٢٠٢٣، ص١١٢.

([٣٨]) المصدر السابق، ص١٥٩.

([٣٩]) المصدر السابق، ص٧١.

([٤٠]) نور الدين بسعدي، دعونا نتحدث عن حماية البيانات الشخصية في منطقة الشرق الأوسط وشمال إفريقيا!، مجلة رؤية الصادرة عن معهد جوته الالماني على الرابط:

https://www.goethe.de/prj/ruy/ar/kuq/24413647/

([41]) Adrian Shahbaz, Allie Funk and Andrea Hackl, Op. Cit, p.1.

([42]) Radio Free Europe/Radio Liberty ©, Iran Blocking Access to 5 million Websites November 21, 2008.

([٤٣]) الفقرة (١) من المادة (١٤) من العهد الدولي للحقوق المدنية والسياسية لعام ١٩٦٦.

([44]) Alaa Kulaib, Egypt's Personal Data Protection Law (PDPL) and where it stands according to the international standards, Association of Freedom of Thought and Expression, p.18.

([45]) Marwa Fatafta, Egypt's new data protection law: data protection or data control? 24 SEPTEMBER 2020, at:

https://www.accessnow.org/egypts-new-data-protection-law-data-protection-or-data-control/