مسؤولية الدولة عن توطين البيانات الشخصية لرعاياها في إطار القانون الدولي لحقوق الانسان

أ.م. د أنسام قاسم حاجم
كلية الامام الكاظم عليه السلام للعلوم الاسلامية الجامعة/ اقسام بابل

The state's responsibility to localize the personal data of its citizens within the framework of international human rights law

Asst.Prof.Dr.Ansam Qasim Hajim Al-Aboudi
Imam Al-Kadhim University College of Islamic Sciences, peace be upon him, Babylon Departments

Abstract:

Countries have moved towards localization laws to protect the digital data of their citizens, to keep pace with technological development and control its effects, which places on the state a legal responsibility under international human rights law to balance its powers with the rights and freedoms of its citizens on the one hand, and between providing technological structures that guarantee the protection of that data within State borders and protecting their owners.

الملخّص:-

اتّجهت الدول نحو قوانين التوطين لحماية البيانات الرقمية لمواطنيها، لمواكبة التطور التكنلوجي والسيطرة على آثاره ، الامر الذي يُلقي على عاتق الدولة مسؤولية قانونية بموجب القانون الدولي لحقوق الانسان، للموازنة بين سلطاتها وبين حقوق رعاياها وحرياتهم من جهة، وبين توفير البنى التكنلوجية التي تضمن حماية تلك البيانات داخل حدود الدولة وحماية أصحابها.

المقدّمة:-

تعدّ البيانات الشخصية والحق فيها وفي حمايتها وسريتها من الحقوق الشخصية اللصيقة بالأفراد، التي ركزّت الوثائق الدولية على صيانتها وكفالة حمايتها، وألزمت الدول على وضع الاليات القانونية التي تبرّئ مسؤوليتها اتجاه تعرّضها للانتهاك، وفي ضل سياسية التوطين التي انتشرت في كل دول العالم لمواكبة التطور التكنلوجي ، واتساع العالم الافتراضي، أصبحت الحاجة متزايدة الى حماية تلك البيانات، الامر الذي يستوجب البحث في هذا الموضوع لمراعاة التوزان بين الحق في حماية وسرية البيانات الشخصية وبين مدى استخدام الدولة لسلطتها في توطين تلك البيانات دون أن يكون هناك انتهاك لها من ناحية.

أهمية البحث: إنّ اهمية البيانات الشخصية لا سيّما إنّ بعضها تعدّ بيانات حساسة ومهمة للدولة، اصبحت اليوم هاجسًا أمنيًا لكلّ دولة ، وأهمية مواكبة التطور في توطين تلك البيانات في ظل الحوكمة الالكترونية، جعلت

Article history
Received: 21/5/2024
Accepted: 26/6/2024
Published: 30/6/2024
تواريخ البحث
تاريخ الاستلام:21 /5/ 2024
تاريخ القبول:26/6/2024
تاريخ النشر:30 /6/ 2024

الكلمات المفتاحية:(التوطين، البيانات، مسؤولية الدولة، القانون الدولي لحقوق الانسان).
Keywords: (localization, data, human rights, state responsibility, international human rights law).

© 2023 THIS IS AN OPEN ACCESS ARTICLE UNDER THE CC BY LICENSE

http://creativecommons.org/licenses/by/4.0/

Corresponding author:
Ansam2hachim@gmail.com

DOI:
https://doi.org/10.61710/vkqt5h06

تلك البيانات شبيهةً بمادة النفط بالقيمة الاقتصادية والتجارية، الامر الذي جعل تلك البينات عرضة للمخاطر وبالتالي تستوجب الحماية فضلاً عن تأثيرها على سيادة الدولة الرقمية، فضلاً عن إنّه لن يتمّ البحث في هذا الموضوع سابقاً.

مشكلة البحث: وفقاً لقواعد القانون الدولي العام لا سيّما القانون الدولي لحقوق الانسان، إنّ الدولة بالوقت الذي تلتزم بتوفير الامن والطمأنينة لرعاياها، بالوقت الذي يقع عليها التزام بحمايتهم وحماية ما يتعلق بهم كبياناتهم الشخصية، الامر الذي يثير تساؤلات اساسية ، تتمثل بمدى حق الدولة بتوطين تلك البيانات؟ وهل يتوافق ذلك مع القواعد الدولية لحقوق الانسان؟ لا سيما مع واقع دولة جمهورية العراق، المتمثل بفتح الباب على مصراعيه أمام التطور التكنلوجي دون وجود غطاء قانوني لتنظيم استخدامه اولاً ولحماية مستخدميه ثانياً، الامر الذي جعل اغلب الافراد يبنون تصورًا بأنّهم دروع بشرية في عالم افتراضي.

منهج البحث وهيكليته: للتوصل الى نتائج قانونية تعالج الاشكاليات الاساسية للبحث، أفضل منهج يعتمد في هذه الدراسة هو المنهج التحليلي بشكل أساسي فضلاً عن المنهج الاستقرائي، وسيتم البحث في هذا الموضوع من خلال مبحثين، سيبحث في الاول تعريف توطين البيانات الشخصية والقيمة الذاتية له ، وفي الثاني تصادم سياسة التوطين مع القواعد الدولية لحقوق الانسان .

المبحث الاول

الإطار المعرفي لتوطين البيانات الشخصية

بداية إنّ المفهوم الاولي لعبارة التوطين لدى الاغلبية مرتبطة عادة بقيام حكومات الدول بتوطين رواتب الافراد ودفعها عبر وسائل الدفع الالكتروني، مسايرة للتطور التكنلوجي، الا انّ ما يتحدد به بحثنا هو النظام القانوني بما يتضمنه من قوانين وتعليمات تصدرها الدولة، تلزم بموجبها الشركات الالكترونية الكبرى مثل" كوكل ومايكروسوفت "، بأن تعالج بيانات المشتركين الخاصة في حدود دولهم ولا تتجاوزها، وليس في الخادم أو الحاسب الذي يسمّى سيرفر(Server)، وحصول موافقة الدولة عند تحويل بيانات الشخص الى طرف آخر سواء أكانت داخل أو خارج إقليمها وحماية تلك البيانات داخل إقليمها(م/1/ و م/ 14من قانون حماية البيانات الشخصية المصري) ، وهذا ما سيتضح في المطلبين الآتيين:-

المطلب الاول

تحديد معنى توطين البيانات الشخصية

لغرض الوصول إلى معنى قانوني لعبارة توطين البيانات الشخصية، لابدّ بداية من تحديد معنى البيانات، كون التوطين كمفردة لا يوجد تعريف لها في القانون.

ويقصد بالبيانات لغةً " مشتقة من بين، أي إخراج الشيء من حيز الاشكال الى حيز التجلي، وما يتبين به الشيء من دلالة" (الرازي، 1987)، وتعرفها المعاجم العربية بأنّها " البيانات الخام التي يشتغل عليها الحاسوب و تتكون من تعبير رقمي وغير رقمي عن أحداث أو حقائق ماضية او مقبلة بقصد تخزينها ومعالجتها للحصول على نتائج محددة" (حبيبي، 2011)، واصطلاحاً تعرّف بأنّها " معلومات تفصيلية حول شخص او شيء ما يمكن من خلالها الاستدلال عليه" (قاموس ومعجم متعدد المعاني والمجالات، 2000)، والشخصية هي" ما يميز شخص معين بذاته عن غيره" فالبيانات الشخصية هي المعلومات التي تتعلق بالأشخاص فتحدد هويتهم، تأخذ شكل أرقام وحروف تتضمن حقائق عن معلومات تمس شخصية الافراد (حسبو، 2000)، فمن خلال تلك البيانات يمكن تحديد هوية الشخص والتعرّف عليه (جبور، 2016)، وتعرف " بأنّها تلك البيانات التي تمت معالجتها لتحقيق هدف معين، او لاستعمال محدد لأغراض اتخاذ القرارات، اي هي تلك البيانات التي اصبح لها قيمة بعد تحليلها او تفسيرها، او تجميعها في شكل ذي معنى والتي يمكن تداولها وتسجيلها ونشرها وتوزيعها في صورة رسمية او غير رسمية " (جبور، 2016).

وتعرف البيانات الشخصية كذلك بـ " مجموعة الحقائق التي تكون عادة على هيأة ارقام او حروف ؛ كبيانات البطاقة الشخصية، ومادة استيفاء النماذج، وقراءة اجهزة الاستقبال " (خشبة)، وتعرف "بأنها

مجموعة المعلومات التي تمس الانسان في شخصه " (حسبو، 2000)، وعرفتها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، بأنّها" كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات كالأرقام والحروف والرموز وما اليها" (م/2/ 3 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، والتي صادق عليها العراق بموجب قانون رقم (31 لسنة 2013، والمنشور في الوقائع العراقية عدد (4292) في 30 ايلول عام 2013) ، كما عرفت " م/ 3/د من البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الإلكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية، 2022 "، "البيانات الشخصية " معلومات متعلقة بشخص طبيعي محدد أو يمكن التعرف عليه " و م/ 1 من قانون حماية البيانات المصري رقم /151 لسنة 2020 عرفت " البيانات الشخصية :أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية . " **و"البيانات الشخصية الحساسة :**البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية "البيومترية" أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة" , ونقطة جيدة باحتساب بيانات الاطفال من الحساسة."

وم/ 1 من قانون حماية البيانات الاردني رقم/24 لسنة 2023نصّت " البيانات الشخصية: 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" .

" البيانات الشخصية الحساسة:" 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 أو أي معلومات أو بيانات يقرر المجلس اعتبارها حساسة إذا كان افشاؤها أو سوء استخدامها يلحق ضررا بالشخص المعني بها."

وفي ضل استخدام الشبكة المعلوماتية فإنّ كل نشاط يقوم به الفرد على تلك الشبكة سواءأكانت تعلق تسجيل الدخول الى موقع الكتروني، او مشاهدة فيديو أو ممارسة العاب ترفيهية أو كتابة تعليق على منشور في وسائل التواصل الاجتماعي، فإنّه يشكّل بيانات تشير الى الشخص نفسه مثل اسمه، عمره، ومكان سكنه، وعدد افراد أسرته، ومركزه المالي والخ، وتستخدم البيانات الشخصية في عدد من الابواب، منها المعاملات الورقية والالكترونية ومواقع التوصل الاجتماعي والاتصالات، وهي بيانات متعددة، قد تكون فردية تتضمن الاسم والعمر والديانة والجنسية والديانة البصمة فصيلة الدم فضلاً عن الصورة والحالة الاجتماعية، وقد تكون بيانات شخصية حساسة تشمل معتقدات الشخص وآرائه السياسية وانتماءاته العرقية والدينية وصحته البدينة والعقلية وسجله الاجرامي، وقد تكون بيانات أرقام شخصية تشمل رقم الهاتف والرقم الوطني الذي تمنحه الدولة لكل فرد من رعاياها بشكل خاص، ورقم البريد الالكتروني رقم سيارته ومنزله ، وقد تكون بينات مالية تحتوي على رصيد الفرد ودخله لشهري، ويدونه وبطاقاته الائتمانية وحسابه المصرفي، واخيراً البيانات الصحية وتشمل بيانات الفرد الصحية وتقاريره الطبية والنفسية والسوابق الصحية (Millard , 1985) ، فتلك البيانات مثل الضرائب والاملاك او التوجهات السياسية والدينية بعد ان كانت معرفتها حكراً على الدولة وصاحبها، اصبحت تلك البيانات ولاسيما المتعلقة بميول الشخص واذواقه الان عرضة للجميع ومباحة ولا سيما للشركات الالكترونية، مثل شركة "Meta" التي تملك تطبيقي "الفيسبوك و الإنستغرام "، التي تشترط لممارسة التطبيق تسجيل تلك البينات .

فالبيانات الشخصية هي معلومات خاصة لكل فرد تتعلق بشؤونه الخاصة وبذاته، ملزمة الدولة بتوفير الحماية لها، انطلاقاً من احترام الحق في الخصوصية ، وبذلك حرصت الدول على حمايتها انطلاقًا من

حماية واحترام الحق في الخصوصية، من خلال تجريم كل فعل من شأنه ان ينتهكها، فالمشرع العراقي جرّم إفشاء الاسرار في المواد(437- 438 من قانون العقوبات العراقي رقم 111 لسنة 1969).

أمّا التوطين لُغةً على وزن "تَفْعِيل"، ويعني: "الجذر" و "وطن" " وطَّن الموضعَ" أي؛ اتخذه وطنًا، و "ووطَّن نفسَه على الأمر" أي؛ حملها عليه" (الحميري ، 1999) ، أمّا تعريف توطين البيانات اصطلاحاً فيعني العملية القانونية التي تقوم الدولة بموجبها بإلزام الشركات الالكترونية التي يعتمد عملها على حفظ البيانات الشخصية للأفراد مثل شركة (Google, Microsoft, Amazon "" ، على حفظ تلك البينات والتعامل بها داخل حدود اقليمها ولا تحولها خارجه الا بعد موافقها (Jennifer Daskal and Justin Sherman, 2020: 3) ، كما عرف بأنّه " العملية التي يصاحبها التخزين لبيانات المستخدم في مراكز مختصة لجمع البيانات على شبكة الإنترنت وذلك داخل حدود الدولة التي تخصها تلك البـيانات(Encyclopedia, data localization, 2021).

ويعني بالتوطين : حماية البيانات من قبل الدولة بدليل اغلب التشريعات الداخلية تستخدم مصطلح " حمايات البيانات"(مثل قانون قانون حماية البيانات الشخصية المصري، قانون حماية البيانات الشخصية السعود ي لعام 2021 وقانون حماية البيانات الشخصية البحريني لعام2018 . قانون حماية البيانات الشخصية الأردني رقم 24لسنة 2023) ، لكن على مستوى القانون الدولي يستخدم مصطلح توطين وهو الاصح ، كون الدولة ملزمة بحماية حقوق رعاياها وبياناتهم لا سيّما الشخصية من خلال توطين معلوماتهم داخل حدود الوطن ، وليس خارجه، فالتوطين يشمل كافة الاجراءات القانونية التي تتخذها الدولة لحماية بيانات رعاياها الشخصية، من ان يمارس بحقها أية نشاط خارج حدود الدولة (Ursic, Nurullaev, & Cuevas, 2018)(، فهي تشمل كل الاليات والبرامج التي تقوم بها الدولة، لإدارة البيانات الشخصية للأفراد التابعين لها، أيًّا كان نوع تلك البيانات، فضلاً عن معالجة البيانات المتعلقة بمؤسساتها، ويجب الامتثال لتلك الاليات والبرامج داخل النطاق المادي للدولة، وهو الامر الذي يستوجب التمييز بين البيانات الشخصية والحساسة والمهمة (Sheppard, Yayboke, & Ramo, 2021)

وهنا نشير الى أنّ دولة العراق خالية من قانون حماية البيانات او أي نص قانوني يشير صراحة الى توطين البيانات، ماعدا قانون البطاقة الوطنية الموحدة رقم/3 لسنة 2016، الا أنّه جاء قاصراً على بيانات محددة وهي " المعلومات المدنية : ما يتضمنه القيد المدني المسجل وفقا لأحكام هذا القانون من الصفات الطبيعية والشخصية والعائلية التي تميز الشخص عن غيره وتحدّد مركزه بأسرته. " (م/1/عاشراً)، ونصّت الفقرة/ سادس وعشرون من م/ 1 من القانون على تعريف " - الشبكة المحلية : إحدى الوسائل الالكترونية التي يستخدمها نظام معالجة المعلومات لنقل البيانات بسرعة عالية ضمن مساحة جغرافية محددة ، ولأفراد لديهم صلاحية الاستخدام ، وتربط هذه الشبكة مجموعة من محطات العمل تحدد وتدار تحت إشراف المديرية العامة ، بما يتيح لها تبادل المعلومات ، ولا يجوز بأي حال من الاحوال ارتباطها هي أو أي من وسائلها او وسائطها بالشبكة الدولية [الانترنيت)"، وهذا يعني مبدئياً أنّ التوطين مقتصر على تلك البيانات بما يتلاءم مع اصدار البطاقة الوطنية " الجنسية " ، الا أنّها وسيلة محلية لا ارتباط لها بمنظومة الانترنت.

فتلك البيانات أيًّا كان نوعها اجتماعية اقتصادية تجارية...الخ تتمّ معالجتها وإدخالها من خلال شبكة الانترنت، الأمر الذي يجعلها لا تقف عند حدود الدولة، بل تنتقل الى أي مكان في العالم، الامر الذي يجعل تلك البيانات متاحة بدون قيود في واقع افتراضي، و مستغلة لمصالح أخرى من ناحية، ومن ناحية يجعل من الصعوبة على الدولة ان تحمي رعاياها من انتهاك الحق في الخصوصية، من خلال السيطرة والرقابة، وبالنتيجة يجعل الامن القومي للدولة متأثر بشكل كبير وسيء، فالتطور التكنلوجي ألقى على عاتق الدولة اعباء من الضرورة معالجتها حفاظاً على السيادة الرقمية للدول والحق في الخصوصية، وعدم تدخل الدول الاخرى في شؤونها.

المطلب الثاني
القيمة الذاتية لتوطين البيانات الشخصية

يثار تساؤل بدايةً الى ان الدولة لو لم تلجأ إلى التوطين ، هل كان يؤثر على التزامها بحماية رعاياها؟ وهل يؤثر على قوتها وسيادتها؟ وهل توطين البيانات الشخصية يعد منهجًا ايجابيًا ام سلبيًا؟

نلاحظ منذ بدأ الغزو التكنلوجي للمجتمع الدولي ، اصبحت كل دولة في تحدٍّ كبيرٍ بين حماية رعاياها وعدم تعرضهم لأي انتهاك، وبين تحصين أمنها القومي ووجوب توفير أمن سيبراني لحماية سيادتها واقليمها، فأصبحت الضرورة تستوجب على كل دولة ان تعترف بالسياسة الرقمية وان تحمي سيادتها الرقيمة ضمن حدود رقمية، فالدولة أصبح لها وجودين واقعي وافتراضي، ممّا يستوجب التوازن بينهما.

فالتوطين كبرنامج قانوني أصبحت الضرورة تستوجب اتباعه، بسبب انتهاك الشركات الالكترونية لتلك البيانات حتى وصل الامر الى التجسس، الذي أدّى الى بناء عدم الثقة بينها وبين الدول، كما إنّها استغلت تلك البيانات لأغراض متعددة منها التجارية مثل معرفة السلوك الاستهلاكي والسلع المفضلة من الافراد، وهذا ما يلاحظه اغلب مستخدمي الفيسبوك مثلاً، مجرد أن تكتب تعليقًا تستفسر به عن بضاعة معروضه وإذا بالمنشورات تنهال عليك عن بضائع مشابه، وقد تم ادانة شركة " ميتا Meta " المالكة للفيسبوك والأنستغرام " بسبب الاستخدام غير المشروع للبيانات لأغراض تجارية مرات عدة، واخر إدانة كانت من قبل الاتحاد الاوربي عام 2022، بسبب استخدامها البيانات بطريقة تخالف قوانين التنافس التجاري(ينظر: الخبر على الموقع الإلكتروني الرسمي لقناة العربية الإخبارية) ، وقد تستخدم لأغراض سياسية للتأثير في الآراء السياسية للأفراد أو استغلالها لحملة دعاية انتخابية، مثلما ادينت شركة " ميتا Meta " عام 2018 ؛ بسبب نقل بيانات (سبع وثمانون مليون) مشترك الى شركة استغلتها في حملة الدعاية السياسية للرئيس الأمريكي السابق" دونالد ترامب"(ينظر: الخبر على الموقع الإلكتروني الرسمي لقناة الجزيرة الإخبارية 21 مارس 2018)، واخيراً قد تستخدم لأغراض التجسس وهي أخطر استخدام كونها تثقل كاهل الدولة وتضعفها، من خلال السيطرة على البيانات العسكرية والبيانات السريّة ، حيث كشفت التسريبات التي أعلنها المتعاقد في وكالة الأمن القومي الأمريكي إدوارد سنودن عام 2013، عن تعاون شركات الكترونية مع الجهات الأمنية الأمريكية في مراقبة بيانات شخصية وحساسة والاطلاع عليها (Swire, Kennedy-Mayo, & Bagley, 2023)

وتوجد برامج تستخدمها الدول للسيطرة على دولة ما ، مثل برنامج **"PRIS** " الذي استخدمته وكالة الأمن القومي الأمريكية لأجل جمع البيانات من برامج الكترونية مثل ،("Google"، " "Microsoft، Facebook "، " "Yahoo" "، YouTube") لذلك عدّ المجتمع الدولي اتباع توطين البيانات، يهدف الى دفع التهديدات عن الدولة، كونه يشترط أن يتم تخزين البيانات داخل حدود الدولة وفق الخوادم المركزية، ومنع انتقالها للخارج لأجل ضمان سريتها وعدم الاضطلاع عليها، كما ان استخدام التوطين سيغني عن متاعب الكابلات الضوئية والتي تسهّل عمل مخترقي النظام الشبكي، وهو ما قد يتسبب في أزمات سياسية وأمنية بين الدول بعضها بعضًا. (Vivekananda, 2018)

كما أنّ سرعة الحصول على المعلومات التي تحتاجها السلطات القضائية لتلبية السرعة في حسم الدعاوي المتعلقة بالجرائم المنظمة، لا سيّما تلك المتعلقة بغسيل الاموال والفساد والإرهاب، جعل التوطين وسيلة مهمة تساعد في ذلك، وبالتالي تخطي صعوبة طلب الحصول على تلك المعلومات من دول اخرى تُخَتَزن فيها تلك البيانات ، الذي كان مصحوباً غالباً بالرفض لإجراءات الخصوصية الصارمة، فضلاً عن الطلب يجب ان يكون مصحوباً بإيضاح الغرض من الحصول على تلك البينات، وهذا يمنح الدول الحافظة للبيانات مجالًا للتدخل بشؤون الدولة صاحبة الطلب، فبالتالي توافر خوادم وطنية داخل حدود الدولة لتوطين البيانات الشخصية وغير الشخصية المهمة ، يُسهّل عمل السلطات القضائية والقانونية فيما يتعلق بجمع أدلة الإثبات و الإدانة، لكن تجدر ملاحظة انه في اطار معنى التوطين، فأن نقل تلك البينات الى داخل إقليم الدولة لا يعني ان ملكيتها تكون قاصرة على الدولة، بسبب كون الجهة المسؤولة عن التخزين والمعالجة المحلية تبقي نفسها، وهي جهات تقديم خدمات الإنترنت التي لن تبيح للدولة أن تمتلك خوادم التخزين؛ لأنّها ستبني خوادمها الخاصة بالتخزين في الدولة المالكة

للبيانات، وإذا تملكتها لن تكون جهة الرقابة على تلك البيانات، ومنه ستضطر الدولة لاتّباع الاجراءات المعقدة للحصول على البيانات الخاصة (CORY & DASCOL, 2021) ،كما أنّ الدولة إذا كانت حريصة على تأمين تلك البينات والوصول إليها بسهولة وامان متشدد فإنّ التوطين لا يحقق غايتها، لذلك بعض الدول تلجأ الى إبرام معاهدات ثنائية لضمان الوصول الى تلك البيانات بشكل خالٍ من القيود ضامن لتحقيق العدل القانوني، مثل قانون 'cloud' الأمريكي الذي أعطى لكل دولة طرفًا في معاهدة مبرمة مع الولايات المتحدة الامريكية امكانية الوصول الى المعلومات الخاصة بها (Malcolm & Panday, 2018).

كما أنّ الدوافع الاساسية التي دفعت الدول الى توطين بيانات رعاياها، هو التحصين ضدّ التدخل الخارجي في شؤون الدولة وفق ما جاء به ميثاق الامم المتحدة، إذ إنّ تلك البيانات عرضة للمراقبة من قبل الدولة التي تستقبلها والتي تشكل الموطن الأم للشركات التي تحضن تلك البيانات، فالدولة لكي تسيطر على إدارة شؤون اقليمها ومن عليه، تملك الحق في الاطلاع على بينات رعاياها أيًّا كان نوعها، الا أنّ الدول الاخرى قد تستغل تلك البيانات لكي تحقق مصالحها من خلال الوصول الى تلك البيانات لإثارة الفتن والطائفية وزعزعة الامن والاستقرار وهذا بحد ذاته تدخل سافر يهدّد الامن القومي للدولة، ناهيك عن استخدام تلك الدول للبيانات التجارية والاقتصادية والامنية التي تمّ توطينها من خلال نقلها الى الخارج، فهذا يعني أنّ الدولة وأسسها اصبحت مباحة ومعرضة لكثير من التدخلات مثل ضرب عملتها والتجسس وضرب نظامها الامني من خلال الارهاب الالكتروني (Wu, 2021) ، فوضع الدولة تدابير أمنية للتوطين توفر تأمين البينات الحساسة لها ولرعاياها من اطلاع الوكالات الاستخباراتية، كون تخزين تلك البيانات داخل دولة معينة يسهل من الاطلاع عليها ومراقبتها لأغراض الامن القومي، ولكن حرصت الدولة على تخزين تلك البينات داخل اقليمها ومنع انتقالها خارجه، فإنّها تضمن تعقيد الوصول إليها، فصحيح ذلك لا يحقّق حماية كاملة لكن عملية الوصول إليها ستكون مكلفة ومعقدة جدا (Hill, 2014).

وكثير ما يستخدم الافراد برامج الكترونية لإيجاد موقع معين او لتسجيل الدخول الى موقع ما، ويتم تحديده وفق الاتصال بالأقمار الصناعية (التي يتم توجيهها لتصوير المواقع اللوجستية للدولة أو توجيه ضربات استباقية) ،وتزويدها بمعلوماته ومنه لتحديد الموقع المراد الوصول له، كما يتم عند استخدام شركةgoogle earth' ، ولو نظر للأمر من زاوية خطورة تقديم شروط تتعلق ببيانات ومعلومات الموقع و تفاصيله ، وكافة المعلومات التي تفيد الفرد الأجنبي مرتاد الدولة، فإنّها تهدّد الأمن القومي للدول المستهدفة من خلال الوصول الى مواقع مهمة (Selby, 2017)

فتوطين البيانات يهدف الى دفع تلك التهديدات عن الدولة، من خلال تخزين تلك البيانات داخل إقليم الدولة على خوادم مركزية، ومنع انتقالها خارج الاقليم للحفاظ على سريتها وعدم الاطلاع عليها، وهناك دول فرضت ضوابط لتخزين تلك البيانات وذلك لاعتبارها معلومات سرية للغاية وتمثل تهديد صريح لأمن الدولة القومي, وسيادتها من خلال تتبع الموقع ببرامج تابعة لأنظمة معينة، لا سيّما أنّ اكتشافات" سنودن " وثّقت أنّ الولايات المتحدة الأمريكية كان لها منفذ للوصول للبيانات تخطّى بدوره حدودها الوطنية، بل وأضاف أن شركات 'google', 'yahoo ، قد مكنّت وكالة الأمن القومي الأمريكية من الوصول إلى بيانات مستخدميها، لذا جاءت تدابير توطين البيانات لأجل حماية البيانات من الوصول غير المشروع (CORY & DASCOL, 2021)

فإنشاء مراكز لتخزين البيانات داخل الدولة، وإنشاء شبكات انترنت منفصلةً عن الإنترنت العالمي، سيضمن عدم تعرض البيانات لهجمات إلكترونية، وهو ما قصدته دولة" ألمانيا"، عندما طلبت من" الاتحاد الأوروبي " إنشاء شبكة إنترنت داخلية تخضع لرقابة وسيطرة "الاتحاد الأوروبي" لحجب التجسس الأمريكي على البيانات الألمانية والأوروبية (Swire, Kennedy-Mayo, & Bagley, 2023) ، إلا أنّ الواقع كشف أنّه في حالة ضعف المنظومة الالكترونية في الدولة سيزيد من مخاطر اختراقها، والهند أكثر مثال على ذلك فرغم تركيز الدولة على صعوبة تقييد البيانات وتكثيف إجراءات الحماية، واقرارها قانون حماية البيانات الشخصية، لتسجل (52974)جريمة عام 2021 بعد أن كان عددها يقدّر ب (44564 جريمة الكترونية سنة 2019) (Basuroy, 2022)، الامر الذي يحتم على

الدولة ان تدعم البنى التحتية التكنولوجية عند توطين بياناتها ولا سيما المتعلقة برعاياها، وحماية نظامها الرقمي (Wu, 2021)

إنّ لجوء الدولة الى التوطين البيانات لرعاياها مطلب ضروري من أجل مواكبة التطور ولتعزيز سيادتها بمفهومها الرقمي، إلّا أنّ ذلك التوطين جعل الدولة امام مواجهة تدخل الدول الاخرى في فضائها الالكتروني؛ بسبب التدفق غير المقيّد لتلك البيانات في الفضاء الالكتروني، فلا بدّ من تخزين تلك البيانات داخل إقليم الدولة والسيطرة عليها، من خلال فرض شروط صعبة على مزودي خدمات الإنترنت، وتقييد انتقالها للدول الأجنبية للمعالجة والتخزين ،لأنّ تخزين البيانات على خدمات "الحوسبة السحابية" لدولة أجنبية يجعل سيادة الدولة منقوصة وخاضعة لرقابة وضغط الدول بشكل مستمر هذا ما يهدّد الأمن القومي والمعلوماتي للدولة المعنية (CORY & DASCOL, 2021) .

المبحث الثاني

تصادم سياسة التوطين مع القواعد الدولية لحقوق الانسان

إنّ لرعايا الدولة حقوق وإنّ على سلطات الدولة التزامات تجاه الأفراد باتخاذ إجراءات من أجل حماية الفرد ممّا يمكن أن يناله من انتهاك لحقوقه والتمتع بها، و إنّ لكل شخص حياته الخاصة وأسراره، التي لا يجوز الاطلاع عليها مطلقاً دون إذن (الحلو، 2005)، وهذا هو الحق في الخصوصية الذي يعرف بأنّه " تــأمين الفرد في حرمة حياته الخاصة سواء ما تعلق بأحاديــثه أم بالأوضاع التي يتخذها لنفسه في حياته الخاصة ، وهو ما يستلزم تجريم كل حصول غير قانوني على حديث خاص أو صورة خاصة " (ابو عامر، 1979)، و اهم قسم في هذا الحق هو المتعلق بخصوصية المعلومات وهو ما يتأطّر به بحثنا، الذي يعرف بـ " حق الافراد والمجموعات والمؤسسات في أن يحدّدوا لأنفسهم متى و كيف وإلى أي مدى يمكن للمعلومات الخاصة بهم أن تصل للآخرين؟ " ، كما عرفه الفقيه (آرثرميلر) بأنّه " حق الفرد في التحكم بانتشار المعلومات الخاصة به " (صالح ، 1993) .

وقد أصبحت جميع المعلومات حتى الوثائق الشخصية والرسائل وكذلك الصوت والصورة تحت تصرف العامة ، بسب التقدم التكنلوجي وزيادة استخدام الانترنيتً ، هذا ما يشكّل خطراً على الحق في الحياة الخاصة ، ممّا جعل التشريعات الجنائية ترسم طريقًا لتوازن بين جميع تلك الحقوق دون المساس بجوهرها . (سرور، 1995) وتعد خصوصية المعلومات من العناصر المهمة والاساسية للحق في حرمة الحياة الخاصة ، إذ إنّ توفير الطمــأنينة وراحة النفس للإنسان في حياته الخاصة ، تقتضي أن يكون للمرء حقه في كتمان أموره الخاصة عن الغير، لاسيما اذا كانت سريّة أو شخصية محضة، ويمنع افشاءها وذلك بالمحافظة عليها. (المحمصاني ، 1979) ، وتزايدت اهمية خصوصية المعلومات بسبب التطور، فاصبح بالإمكان الحصول عليها بسهولـــة ، بوساطة شبكــة المعلومـــات الدوليـــة " الانترنيت" ، مما تطلب تدخل الدولة بشكل قانوني لحمايتها، و يمكن للدولة ان تضع قيود قانونية على هذه الخصوصية ، متى ما وجدت الدولة ان الافراد كالأجانب أو الجواسيس أو المشبوهة بهم ، تشكّل تحركاتهم وتصرفاتهم خطراً على أمن الدولة وسلامتها، ممّا يؤدي بالقانون إلى اجازة مراقبة خصوصياتهم (المحمصاني ، 1979)، الامر الذي يستدعي البحث في آلية الدولة في التوطين في ضوء الالتزامات الدولية، ومدى علاقتها بحقوق الانسان في القانون الدولي.

المطلب الاول

آلية التوطين الداخلية للدولة في ضوء التزاماتها الدولية

لقد أصبحت خصوصية المعلومات في وقتنا الحاضر من الامور المهمة التي تستوجب تكثيف الحماية لها، بسبب التطور التكنلوجي الذي وفّر سرعة وسهولة الحصول عليها، وإن الحق في الخصوصية إطار عملية توطين البيانات، تعني إمكانية الفرد في مشاركة معلوماته الخاصة مع مقدمي

خدمات الانترنت للحصول على تلك الخدمات، لذلك يُرى ان تلك المشاركة وانتقال تلك لبيانات عبر حدود الدولة هو انتهاك لذلك الحق وخرق لكيان المجتمع في داخل دولة ما، وإنّ أفضل وسيلة لتفادي ذلك هو اتباع سياسة التوطين التي تركّز على نطاق حفظ التعامل مع تلك البيانات يكون في حدود الدولة لا خارجها، واعطاء الفرد السلطة الكاملة في معالجتها والتحكم بها استناداً الى مبدأ " حق تقرير المصير المعلوماتي للفرد " ، الذي جاءت به نظرية" تقرير المصير للمعلومات الشخصية "التي تمنح الفرد الحق في إدارة بياناته (Hong, 2019) ومن ناحية اخرى سيمنح الدولة إمكانية السيطرة على رعاياها ومراقبتهم وحماية حقوقهم، من خلال الاعتماد على مكان تخزين تللك البيانات، الامر الذي دفع أغلب الدول إلى اصدار قوانين خاصة لحماية البيانات مثل " الهند فرنسا الولايات المتحدة ،كوريا، إندونيسيا، الاردن ،مصر والامارات " (Panday & Malcolm, 2018) .

لكن الامر الذي يجعل عملية التوطين مضرة بحقوق الانسان لرعايا تلك الدولة، هو أنّ أغلب الدول تحرص على تخزين تلك البيانات داخل حدود اقليمها، لكن تهمل الجوانب الفنية والتقنية لتحصينها من الاختراق، إذ إنّ أغلب الدول ومنها العراق لا تملك البنى التكنلوجية التي تتميز بالدقة والتطور المعلوماتي والأمني لتخزين البيانات وحمايتها، بل وحتى إطار قانوني لحمايتها ضعيف جدًا في دولة العراق، فالحفاظ على سرية تلك البيانات لا يتعلق فقط بمكان حفظها بل يتعلق بكيفية الحفاظ عليها، فالشركات الالكترونية المقدمة لخدمات معالجة البينات تمتلك مستوى عالٍ من التقنية والدقة من الصعب اختراقها وهي في تطور مستمر وفقاً لسوق العمل، وإنّ التوطين يقضي على ميزة" التجزئة" ، أي تجزئة البيانات من خلال قواعد تخزين البيانات المختلفة التي تمتلكها الشركات ، وهو ما يحدّ من فرص اختراقها والوصول لها، لكنّ فكرة التوحيد المعلوماتي يسهّل من عمل اللجان الإلكترونية في الوصول لتلك البيانات واختراقها (urban, 2021)، وهنا يُثار تساؤل هل بإمكان الدولة أن تقيّد حق الشركات الالكترونية التي يتم من خلالها تخزين تلك البيانات وتوطينها الكترونياً في التصرف بتلك البيانات؟ هنا الاجابة تكمن حول وجود اتفاق بين الدولة المعنية وتلك الشركات، طالما أنّ العقد شريعة المتعاقدين فهو يخضع لما يتفق عليه الاطراف، فللدولة لها حق فرض التزامات على الشركات العاملة فيها سواء أكانت وطنية أم اجنبية، لكن في حدود معينة، فحماية البيانات يتطلب من الدولة أن تحرص أثناء التعاقد على التركيز على آلية التصرف بها، مع الاخذ بنظر الاعتبار أنّ وجود هذه الشركات خارج اقليم الدولة وبالتالي إخضاعها للقوانين الوطنية يواجه صعوبة كبيرة، فالتوطين يتطلب شراء خوادم جديدة يخزن فيها بيانات رعايا الدولة، او بنقل تلك الخوادم من دول أخرى.

وإنّ موقف الصين من إنشاء مشروع " **Golden shield** " أو الجدار الناري للصين العظيم " ، لمراقبة شبكة الإنترنت وحجب المواقع الضارة، واطلاق أخرى بديلة تجعل كل بيانات الاشخاص والبرامج الالكترونية واستخدامها خاضع لسيطرة ورقابة الحكومة الصينية كمحرك البحث" بايدو"، وموقع" ويبو , (Khalifa) ، فضلاً عن قيام الهند بإغلاق شبكة الإنترنت لعدة مرات ؛ إذ ظهر أنّها اخذت المستوى الاعلى في اغلاق الانترنت ب (106) مرة في عام 2021، وذكرت شركة فيسبوك سنة 2013، في تقرير لها ان دولة الهند طلبت ب (3245) طلب لبيانات لأفراد هنود يستخدمون هذا التطبيق (report, 2022)، كون فكرة ان الدول لا سيّما تلك التي تتميز نظمها السياسية بالاستبدادية تستغل توطين بيانات الافراد، لإحكام سيطرتها على رعاياها والتعديّ على خصوصياتهم، وبالتالي السيطرة على المنافذ الالكترونية لمراقبة مايتداول على الشبكة الالكترونية، للقضاء على المعارضة وتقييد الحريات لاسيّما حرية التعبير، وحجب المواقع التي تهدّد أمن الدولة واستقرارها.

ومن ناحية أخرى شكل التوطين تحدي صعب للجهات الامنية، بسبب استغلال تلك البيانات من قبل جهات غير قانونية لإثارة الطائفية والترويج للأفكار المتطرفة والتشجيع على التجنيد والانضمام الى جماعات ارهابية كـ" جند السماء وتنظيم داعش الارهابي "، حيث تشن هجمات الكترونية من قبلهم لتستولي على بيانات ومعلومات شخصية أو سرية، ومن ثم دراسة الهدف والتخطيط لتجنيده عبر استهداف فكره ومعتقده وآراءه، وبالتالي اتاحة كل البيانات بصورة سهله يحول رعاياها خلايا نائمة لخدمة العناصر المشبوهة، واخيراً يدق جرس الخطر والتهديد لأمن الدولة (Griffiths, 2023).

وفي ضوء ما تمّ ذكره في هذا المطلب يتضح أنّ التوطين سلاح ذو حدّين، فصحيح يمكن الدولة من خلال التوطين أن تنفّذ قانونها، وتعزّز أمنها وسيادتها الالكتروني في ظل التطورات التكنلوجية, الا أنّها تجعل الدولة امام مسؤولية كبيرة من حيث تجاوزها بمراقبتها حدود صلاحياتها، أو استغلالها سيطرتها على المعلومات ومراقبة المحتوى المقدم للأفراد على البرامج الإلكترونية لا سيّما الدول التي تتبنى أنظمة استبدادية، فتشل المعارضة وقمع الحقوق والحريات، فإذا كان التوطين غرضه منع الوصول الى بيانات الافراد من قبل الدول الاجنبية الا من الدولة نفسها، فان الدولة ممكن ان تستخدمه كأداة للوصول غير المشروط لبيانات مواطنيها، لتصبح بالنتيجة بيانات رعاياها خاضعة " للاستعمار الرقمي المحلي ".

ومن ناحية اخرى إنّ الدولة مسؤولة عن كل خطر يتعرض له رعاياها ،بسبب سياسة التوطين ولا يسيما اولئك الذين يشغلون مناصب حساسة ويقومون بمهام اساسية في الدولة ، فلو اخذ على سبيل المثال إجراءات الاتحاد الاوربي في التوطين، الذي وضع اللائحة العامة لحماية البينات 'BGDR ،التي فرضت شروط صارمة على انتقال البيانات خارج حدود الاتحاد الأوروبي، فاشترطت الانتقال للتخزين والمعالجة مقيد بتوفر تقنيات متطورة ومعقدة لتأمين وحماية تلك البيانات، وحتى نقلها لدولة أخرى لكي تتم يجب أن تتوفر فيها معايير الحماية والخصوصية المتبعة من قبل دول الاتحاد الاوربي، وعملت نموذجًا لمراكز البيانات داخل الاتحاد الأوروبي، ضمن مبادرة ألمانيا لمنطقة" شنغن"، وذلك لحماية البيانات الحساسة غير القابلة للانتقال خارج حدود الاتحاد الأوروبي واعطت للفرد استخدام " مبدأ تقرير المصير المعلوماتي" أي الحرية والحق في تقرير تسليم ب، وتطبيق قانون الدول الاوربية خارج حدود الاتحاد، بياناته الشخصية والاذن باستخدامها (General Data Protection Regulation, Regulation (EU) , 2016) ، وقد اتبعت نسبة منه اغلب الدول منها (استراليا وفيتنام ونيجيريا وتركيا ومصر والاردن والبحرين)، الامر الذي يثير تساؤل عن حجم الخطر الذي يهدّد دولة العراق ورعاياها في ظل اتباع سياسية التوطين بدون اجراءات حماية قانونية ولا بنى تكنلوجية متطورة، حيث لغاية كتابة هذا البحث لا يوجد قانون يضمن اجراءات الحماية والحياة الالكترونية في العالم الافتراضي ، ماعدا نص في دستور العراق لعام 2005، التي اعطت الحق في الخصوصية لكل فرد بما لا يتنافى مع الآداب العامة(م/17، اولاً) ، دون ان ينص على حماية ذلك الحق الذي يتبعه الحق في حماية البيانات الشخصية.

المطلب الثاني

مراعاة القانون الدولي لحقوق الإنسان في توطين البيانات الشخصية

إنّ الهدف الأساس من التوطين حماية البيانات الشخصية للأفراد وما يتعلّق بمعالجة بياناتهم الشخصية فضلاً عن الحقوق والحريات الأساسية وعلى رأسها الحق في حماية بياناتهم الشخصية (General Data Protection Regulation, Regulation (EU) , 2016) ، لا سيّما وفي ظل التطور التكنلوجي فإنّ تلك البيانات اصبحت على حدّ تعبير أحدهم هي " النفط الجديد " (Szczepański, 2020)ونصّت م/12 من الاعلان العالمي لحقوق الانسان بـ" لا يجوز تعريضُ أحد لتدخُّل تعسُّفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمسُّ شرفه وسمعته. ولكلِّ شخص حقٌّ في أن يحميه القانونُ من مثل ذلك التدخُّل أو تلك الحملات." م/ 18 منه على " لكلِّ شخص حقٌّ في حرّية الفكر والوجدان والدِّين، ويشمل هذا الحقُّ حرّيته في تغيير دينه أو معتقده، وحرّيته في إظهار دينه أو معتقده بالتعبُّد وإقامة الشعائر والممارسة والتعليم، بمفرده أو مع جماعة، وأمام الملأ أو على حدة. "

وم/ 19 منه على " لكلِّ شخص حقُّ التمتُّع بحرّية الرأي والتعبير، ويشمل هذا الحقُّ حرّيته في اعتناق الآراء دون مضايقة، وفي التماس الأنباء والأفكار وتلقِّيها ونقلها إلى الآخرين، بأيَّة وسيلة ودونما اعتبار للحدود"

وبعد ان شرّعت مصر قانون حماية البيانات الشخصية المصر رقم "151" لسنة 2020، نقده المعنيين بحقوق الإنسان بأنّ الدافع وراء تشريعه هو تمكين الجهات الامنية من الحصول على بيانات

المواطنين والاطلاع عليها في ظل فقدان الرقابة قضائية، مع الإشارة الى انه في مرحلة مناقشته وقبل اقراره اعترض بعض النواب عليه كونه مقيد للحرية ومجرد من الواقعية التي تعالج بها قوانين البيانات الشخصية (محمود، 2023)، وللإجابة عن مدى تأثير التوطين على حقوق الانسان يُلاحظ:

بالنسبة للحق في الخصوصية إنّ التوطين يجعل تلك البيانات تحت تصرف الدولة لاستغلالها بما يحقق مصالحها، كما انها تحتاج الى تقنية متطورة لحمايتها تعجز الدولة احياناً عن توفيرها، ليصل الامر الى هدر ارواح الافراد بسببها، و إنّ الحق في الخصوصية يتمثل في حرية الفرد في انتهاج الأسلوب الذي يختاره ويرتضيه لحياته بعيداً عن تدخل الآخرين من ناحية ،و حق الفرد في إضفاء طابع السرية على الأخبار والمعلومات التي تتولد عن حريته في اختيار حياته الخاصة من ناحية اخرى (عبد الحكم، 2007)، فالحق في الخصوصية هنا هو خصوصية المعلومات ، اي القدرة على السيطرة على المعلومات الخاصة والتحكم فيها ، وهو أهم ما يقصد بالخصوصية في علاقتها بالمعلوماتية (عبد الزغبي، 2006) ،إذ إنّ حياة الفرد الخاصة أمام التطور التكنولوجيا اضحت شفافة وواضحة ، فبالإمكان ترجمة حياة الفرد في أقل من الثانية الواحدة، كما أثرت تكنولوجيا المعلومات على هذا الحق على نحو أظهر إمكان المساس به إذا لم تنظم أنشطة جمع ومعالجة وتبادل البيانات الشخصية الجارية في نطاق نظم معالجة البيانات وخوادم المعلومات، ففيها يتمّ تخزين كل المعلومات عن ملايين الأفراد ، والاحتفاظ بها إلى الأبد واستخراج بيانات كافية في أي وقت عن أي فرد من المسجلين بها ، وتعرية حياته بكشف تفاصيل سابقة على وقت استخراج تلك البيانات بزمن طويل ، وبالتالي تصبح هذه البيانات سهلة المنال ومتاحة للجميع (المكاوي، 2010) .

إنّ استخدام وسائل التقنية الحديثة والعالية في ميدان جمع ومعالجة البيانات الشخصية ، من قبل الدولة أو القطاع الخاص قد وسع من حجم التناقض بين حق الأفراد في الحياة الخاصة ، والحق في الاطلاع عليها من قبل السلطات المختصة ، ويتمثل ذلك في التناقض بين الحق في الخصوصية وحق الدولة في الاطلاع على شؤون الأفراد ، عِبر اطلاعها على البيانات الخاصة بالفرد بشكل يتناقض مع صونها واحترامها ، والتناقض بين حق الفرد في الاحتفاظ بسرية بياناته ، ومصلحته بكشف حياته الخاصة للحصول على فوائد هذا الكشف في حالة استعمالها طوعاً لأغراض مغايرة للتي أعطيت لأجلها، كما في برنامج (tiktok) لسياسته التي تسمح بعرض تلك الخصوصية بشكل يخدش الذوق العام والآداب العامة فقد تمّ حجبه من اغلب دول العالم ماعدا العراق، لدرجة أصبح حقه في حماية شرفه وعرضه مقابل مغريات مادية يواجه صعوبة المحافظة عليه، وفق سياسة هذا البرنامج وللحصول على أعلى نسب مشاهدات ، **واخيراً** التناقض بين حق الحياة الخاصة ، والحق في جمع المعلومات لغايات البحث العلمي وحريته ،وبين حرية الصحافة وتبادل المعلومات وبين موجبات الاطلاع على شؤون الفرد ، بما فيها تلك التي تقع ضمن نطاق حياته الخاصة (فيصل، 2008)) ، وهنا نركز على ان تلك البيانات تستخدم في ارتكاب العديد من الجرائم يصل فيها كثير من الأحيان الأعتداء على حق الإنسان في سمعته أو اعتباره أو شرفه كالقذف والسب والتهديد ، مثل ما قام به حزب العمل المعارض في إسرائيل من نشر صورة عارية لزوجة نتنياهو رئيس الوزراء الإسرائيلي الأسبق على شبكة الإنترنت (الصغير، 2002) .

فبعد أن كانت هذه البيانات في ظل الطرق التقليدية لا يطلع عليها إلاّ صاحب الشأن نفسه بإتباع إجراءات معينة ، أصبح بإمكان أي شخص يمتلك نسبة من الإمكانيات التكنولوجية أن يصل لهذه البيانات، بما ينتهك الحق في الحياة الخاصة بالفرد الذي تتعلق به تلك البيانات، فأن حمايتها تتم بالنصوص الجنائية التقليدية " كحماية الملفات الطبية أو الأسرار المهنية " الا انها لا تغطي حماية شرف الإنسان وحياته الخاصة في الوقت الحاضر الافتراضي.

وان دستور جمهورية العراق لسنة 2005 قد أكد في م/ (17/ أولاً) على أن لكل فرد الحق في الخصوصية الشخصية ، بما لا يتنافى مع حقوق الآخرين ، والآداب العامة، كما ان الحق في حرية التعبير يعد من الحقوق الاساسية التي نص ميثاق الامم المتحدة في م/ 1 على المساواة والتزام الدول باحترام حرية الرأي وممارسة الشعائر الدينية، وكفل العهد الدولي الخاص للحقوق المدنية والسياسية للأفراد حرية التعبير بالنص " "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 "(م/19/ ثانياً) ، 1966، فضلاً عن الاتفاقية الاوربية لحقوق الانسان، والميثاق العربي لحقوق الانسان الذي صادق عليه العراق في 2004(بموجب القانون رقم لسنة 2004 ودخل حيز النفاذ في 2008) وجاء مضمون م/ 38 من دستور 2005 ضامن لهذا الحق بالنص" تكفل الدولة وبما لا يخلّ بالنظام العام والآداب:اولاً .حرية التعبير عن الرأي بكل الوسائل "

وقد لاحظت المنظمات غير الحكومية المعنية بحقوق الانسان ان توطين البيانات الشخصية، يحارب الحق في ابداء الرأي، إذ يُمكن سلطات الدولة من تخزين بيانات الافراد المتعلقة بآرائهم ولا سيما المكتوبة والاطلاع عليها، ومن ثم استغلالها لمقاضاة المعرضين تحت عنوان حماية قيم المجتمع والنظام العام وحماية النظام العام ومحاربة الارهاب، وفي تقرير لمنظمة العفو الدولية عن حالة حقوق الانسان في الدول العربية، ذكرت ان بعض هذه الدول تنتهك حق الافراد في الرأي وتلاحقهم قضائياً ، ففي دولة سوريا يعد انتقاد الحكومة جريمة عقوبتها السجن، وقد اعلن وزير الداخلية السوري عن القبض على (11 مواطن سوري) بتهمة نشر أخبار على مواقعهم في برنامج الفيسبوك (Shahbaz, Funk, & Hackl, 2020).

وبالنسبة للحق في الوصول للمعلومة الذي نصت عليه م/ 13 من العهد الدولي الخاص بالحقوق الاقتصادية ولاجتماعية والسياسية لسنة 1966، و/ المادة/ 34 من دستور العراق 2005" ...، ثالثاً:- تشجع الدولة البحث العلمي للأغراض السلمية بما يخدم الإنسانية، وترعى التفوق والإبداع والابتكار ومختلف مظاهر النبوغ"، وهنا اعتبرت المؤسسات الإعلامية والصحف الإلكترونية بان التوطين سيمكن سلطات الدولة من حجب أي موقع صحفي أو أخباري ، تعتقد الدولة انه يتعارض مع سياستها، حتى لو كان ذو طبيعية ثقافية أو سياسية أو اجتماعية (Shahbaz, Funk, & Hackl, 2020)، ففي دول مثل (الصين وروسيا وإيران)تم حجب الألاف المواقع الإلكترونية ،التي ترى السلطات المختصة انها تتضمن انتقاد أو تقرير يتضمن جوانب سلبية ضد الحكومة، فدولة ايران قامت بحجب أكثر من خمسة ملايين موقع الكرتوني لغاية 2008 (Swire, Kennedy-Mayo, & Bagley, 2023)، ولو نظر الى ما يحصل في دولة العراق يلاحظ وصل الامر الى حجب الانترنت بشكل عام في فترة الامتحانات لمنع تسريب الاسئلة او اختراقها، الذي تسبب بخسائر مادية كبيرة للقطاعين العام والخاص، في الوقت الذي يستوجب على الدولة ان توفر بنى الكترونية مهمة لحمايتها.

ولعل أهم حق تمس به سياسة التوطين في ظل استخدامها من قبل كل الدول، هو الحق في المحاكمة العادلة والحق في المقاضاة لحمايته من التعسف والظلم الذي قد يقع عليه من اجهزة الدولة الامنية، لذلك نص العهد الدولي للحقوق المدنية والسياسية 1966 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" (م/14/ 1 من العهد) ، م/ 8 من الاعلان العالمي لحقوق الانسان، و م/ 19 من دستور العراق 2005 نصت على :...، .ثالثًا التقاضي حق مصون ومكفول للجميع "

ويلاحظ هنا أنّ قوانين التوطين تفتقر الى تنظيم رقابة قضائية ، فقوانين اغلب الدول المتعلقة بالتوطين ومنها (مصر، السعودية، والاردن) لا يوجد فيها طريقة للطعن بالدليل المستخرج من البيانات الشخصية من قبل الجهات الامنية، بل يعطي للسلطة التنفيذية الحق في الاطلاع على البيانات دون اشعار طالما تعلقت بالأمن القومي والمصلحة العامة، وهذه المصطلحات عامة من الممكن ان يدخل في نطاقها حالات لا علاقة بها، وهذا عكس ما اقرته سياسة التوطين في الاتحاد الاوربي ؛ إذ اعطى للأفراد حق اللجوء الى القضاء ومنها المحكمة الاوربية لحقوق الانسان ، التي بإمكانها النظر في قضايا توطين البيانات الشخصية والرقابة عليها والتي قضت بانه من واجب الدولة ان تتخذ الاجراءات اللازمة لحماية الخصوصية لرعاياها فضلاً عن امتناعها عن التدخل فيها دون سند قانوني ، واعطى النظام الاوربي لحماية البيانات الشخصية حق الافراد المتضررين بالتعويض، لذلك يُلاحظ ان التوطين منح

سلطات الدولة صلاحيات كثيرة، ولم يحيط المواطن بضمانات من خلال منح القضاء دورًا في مراقبة تصرفات الحكومة الخاصة بالبيانات الشخصية (اسماعيل، 2019)

فضلاً عن الحق في حياة حرة كريمة الذي نصت عليه م/3 من الاعلان العالمي لحقوق الانسان 1948 بـ " لكلِّ فرد الحقُّ في الحياة والحرّية وفي الأمان على شخصه "، وم/ 15 من دستور 2005 نصت " لكل فردٍ الحق في الحياة والأمن والحرية، ولا يجوز الحرمان من هذه الحقوق أو تقييدها إلا وفقاً للقانون، وبناءً على قرارٍ صادرٍ من جهةٍ قضائيةٍ مختصة" .

وهذا يبدو من الصعوبة تحقيقه في ظل ما يجري في برامج التواصل الاجتماعي ولا سيما في العراق، حيث هناك الكثير من سياسيات هذه البرامج تتعارض مع الآداب العامة والنظام العام لا تتوفر فيها سياسة استخدام قانونية تقيد على اقل تقدير عدم استخدامها من قبل الاطفال فضلاً عن عدم توفر امكانية حجب المواقع السيئة ، مما يأثر بشكل كبير على المنظومة الاخلاقية . وهنا نشير الى انه حددت م/(438) من قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، صور الاعتداء على الحياة الخاصة بشكل حصري، ليس من بينها حماية البيانات الشخصية للفرد في مواجهة البرامج الإلكترونية، والتي يعد استخدامها أو استغلالها في غير الغرض المخصص لها أعتداءً على الحياة والحريات الخاصة للفرد، إذ تنص على أنه" يعاقب بالحبس مدة لا تزيد على سنة وبغرامة ...، : أولاً : من نشر بإحدى طرق العلانية أخباراً أو صوراً أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة إذا كان من شأن نشرها الإساءة اليهم . ثانياً : من اطّلع من غير الذين ذكروا في م/ (328) على رسالة أو برقية أو مكالمة تليفونية فأفشاها لغير من وجهت إليه إذا كان من شأن ذلك إلحاق ضرر بأحد " ، كما ان الفقرة/ ثانياً من م/ 17 من قانون البطاقة الوطنية رقم /3 لسنة 2016 نصت على " ثانيا - لا يجوز لمـن حصل علـــى معلومات وفقا لأحكام هذه المادة ان يستخدمها فـــــي غير الغرض الذي طلبت من اجله." دون ان تحدد عقوبة على ذلك المنع وهذا خلل كبير جداً يحتاج الى اعادة نظر، لاسيما وانها الفقرة الوحيدة التي تضمنت حظر استخدام تلك البيانات بطريق غير مشروع.

وتهدد البيانات الالكترونية الحق في الحياة وهو حق مقدس نصت عليه كل المواثيق الدولية المعنية بحقوق الانسان ، فضلاً عن الدساتير ومنها دستور العراق 2005 فتستخدم كوسيلة لارتكاب جرائم الضرب والجرح و التهديد بالقتل او الاتجار بالبشر ، فعلى أثر مشادة بين شخصين على أحد برامج التواصل الاجتماعي انتهت بمشاجرة في ولاية نيوجيرسي، إذ تمكن المتهم من تتبع عنوان المجني عليه من خلال الإنترنت، ثم اصطحب زملائه إلى هذا العنوان واعتدوا على المجني عليه بالضرب (منصور، 2011).

استناداً الى ما تم بحثه اعلاه نستطيع ان نتوصل الى نتيجة مفادها ان التوطين يشكل تهديداً لكل حقوق الانسان وحرياته، تلك التي رسمها القانون الدولي لحقوق الانسان والزم الدول بكفالة حمايتها، لا سيّما حرية التعبير وحرية المعتقد والدين والحق في الخصوصية .

الخاتمة :-

بعد التوفيق من الله عز وجل, انتهينا من البحث في موضوع (مسؤولية الدولة عن توطين البيانات الشخصية لرعاياها في اطار القانون الدولي لحقوق الانسان) , ووصلنا لعرض اهم الاستنتاجات ,والتوصيات التي تمخضت عنها الدراسة وهي كالاتي:-

1- في ظل التطور التكنلوجي واتساع الحياة الافتراضية، فان الدول امام تحدٍ كبير ومسؤولية، فمن ناحية يجب ان تماشي تطور المجتمع الدولي في الاستخدام التكنلوجي والرقمي ومن ثم ضرورة اللجوء الى سياسة التوطين، ومن ناحية التزامها دولياً بتوفير الحماية اللازمة لرعاياها، وبلا شك عدم التوازن بين هذين الامرين يؤثر على قوة الدولة وسيادتها، كونها تصبح ساحة مفتوحة ورعاياها للجميع.

2- لجأت الدول الى توطين بيانات رعاياها داخل حدود اقليمها للتخلص من سيطرة الشركات الالكترونية الكبرى في معالجة البيانات الشخصية خارج حدود الدولة، الا في حالات استثنائية، ووضعت قوانين لذلك التوطين لغرض حماية بيانات رعاياها وعدم انتهاك حقوقهم، الا ان الواقع أثبت عدم توفر

ضمانات كافية لحماية بياناتهم وجعلها مباحة للأجهزة الأمنية واجازت استباحتها بدعوى حماية الامن الوطني.

3- لا توجد قواعد دولية تحكم عملية التوطين، مما يجعلها خاضعة لمبدأ سيادة الدولة على اقليمها ، الامر الذي يجعل الدولة امام مسؤولية قانونية كبيرة في ضبط الاصول القانونية للتوطين، بما يعزز سيادتها ويحمي رعاياها.

4- إنّ عملية توطين البيانات لا تحتاج الى حصر تلك البيانات في اقليم الدولة حصراً وعدم جواز نقلها الى الخارج، بل تحتاج الى بنية تقنية متطورة وتتطور مع تطور الحياة الالكترونية، فالعبرة ليس في مكان الخزن بل في كيفية الحفاظ على البيانات المخزونة، كونها متاحة بدون قيود في واقع افتراضي، و مستغلة لمصالح اخرى ، الامر الذي يجعل من الصعوبة على الدولة ان تحمي رعاياها من انتهاك حقوقهم، من خلال السيطرة والرقابة، وبالنتيجة يجعل الامن القومي للدولة متأثر بشكل كبير، فالتوطين القى على عاتق الدولة اعباء من الضرورة معالجتها حفاظاً على السيادة الرقمية للدول والحق في الخصوصية، وعدم تدخل الدول الاخرى في شؤونها.

5- اتضح ان دولة العراق بعيدة عن اجراءات التوطين الاساسية فلم نجد اية عملية اجرائية او قانونية متعلقة بالتوطين، حيث سارع مجلس النواب مطلع عام 2011 إلى اقتراح قانون جديد يهدف إلى تقويض استخدام تكنولوجيا المعلومات عبر مشروع أسماه" مشروع قانون الجرائم المعلوماتية "، بالإضافة إلى قانون التوقيع الإلكتروني والتعاقد الالكتروني، هذا وقد تضمن المشروع عقوبات قاسية لمن يستخدم البيانات الرقمية لأجل تقويض استقلال أو وحدة أو أمن الدولة ومصالحها الاقتصادية والعسكرية والأمنية، و أحيل المشروع للبرلمان لأجل قراءته أول مرة في(27/ تموز/2011)، ولكنّه واجه رفضًا شديدًا، كونه يقيد حرية التعبير ويهدد الصحفيين الذين يكشفون وقائع الفساد في البلاد وقد تم إلغائه بالفعل من قبل مجلس النواب العراقي في (2013/2/5) ، فضلاً عن عدم وجود قانون مختص بحماية البيانات في العراق اسوةً بقانون قانون حماية البيانات الشخصية البحريني رقم /30 لسنة 2018، وقانون حماية البيانات الشخصية الأردني رقم/ 24 لسنة2023 ، و قانون حماية البيانات الشخصية المصري، وكل الدول الاوربية.

لا سيّما أنّه لا يجوز قياس جريمة الاعتداء على المعلومات الشخصية من خلال شبكة الإنترنت على جرائم الاعتداء على الخصوصية التي تضمنها قانون العقوبات رقم11 لسنة 1969. كما يلاحظ ان قانون الإثبات العراقي النافذ رقم (107) لسنة 1979 أو عن طريق التعديل رقم (46) لسنة 2000، لم ينظم أحكام أدلة الإثبات الإلكترونية، ممّا يعني فراغ تشريعي، يعانيه الواقع الحالي لا يستظل بالحماية القانونية الكافية التي تحميه شر هذه الجرائم المتطورة ، التي لا يكون محلها أشياء مادية تقليدية تعارف الناس عليها.

6- واخيراً ان التوطين يشكل تهديداً لكل حقوق الانسان وحرياته، تلك التي رسمها القانون الدولي لحقوق الانسان والزم الدول بكفالة حمايتها، ولا سيما حرية التعبير وحرية المعتقد والدين والحق في الخصوصية والحق في الحياة والكرامة وفي اللجوء الى القضاء، اذا ما قامت الدولة بتوفير ضمانات قانونية وتطبيقها في الحياة الافتراضية، إنّ ازدياد الوسائل والبرامج التكنولوجية وتطورها المستمر ادى إلى ازدياد مخاطرها على حقوق الانسان وحرياته حيث أصبحت تقيد الفرد في تنقلاته ، وترصد أعماله وحركاته وتجمع البيانات الشخصية وتخزنها وتعالجها بواسطة الانترنت ، وهي تعكس جميعها تهديداً مباشراً وجديداً على الحياة الخاصة ، خاصة اذا استخدمت لأغراض مختلفة من دون رضا أصحابها الذين لا يكونون أصلاً على علم بوجودها.

التوصيات:-

1- ضرورة السعي الى اعتماد المعايير العالمية في حماية البيانات الشخصية مثل النظام الأوروبي لحماية البيانات لعام 2016، وهذا بدوره والتي سيوفر فرصة جلب الاستثمارات الاجنبية وتحقيق خطط التنمية المستدامة التي يعد العراق في اشد الحاجة اليها.

2- ان بقاء الواقع الافتراضي في العراق على ما هو عليه في ظل الغياب التشريعي سيؤدي الى معدل ارتكاب الجريمة بصورة مرعبة اسوء مما هو عليه الان، لذلك ندعو المشرع العراقي إلى الإسراع بسن مشروع قانون جديد لحماية المعلومات ، وقانون يجرم الجريمة الالكترونية، لا سيما وان القوانين التقليدية عاجزة عن احتواء الظاهرة الإجرامية الالكترونية المستحدثة، وبالتالي فإن عدم وجود نصوص قانونية تجرم وتعاقب على الجريمة المعلوماتية , مكن الجناة من الإفلات من العقاب, وكل ذلك احتراما لمبدأ الشرعية' لا سيّما أنّه لا يجوز قياس جريمة الاعتداء على البيانات الشخصية من خلال شبكة الإنترنت على جرائم الاعتداء على الخصوصية التي تضمنها قانون العقوبات رقم11 لسنة 1969.

3- الدعوة إلى وجوب تأهيل وتوعية القائمين على الأجهزة الامنية على التعامل مع هكذا أمور تقنية بحتة ، لاسيّما في الجانب الدولي ، إذ إنّه ليس بمقدور دولة ما التوفيق والنجاح في مواجهة هذه الأنماط المستحدثة بمفردها دون وجود تعاون وتنسيق مع غيرها من الدول الأخرى من أجل مكافحة هذه الفئة من المخاطر التقنية ، وان تشجيع وتطوير الثقافة الحاسوبية والمعلوماتية بين رجال القانون والشرطة وربطها بالثقافة القانونية يكفل للأجهزة الأمنية والسلطات تحقيق النجاح الكبير في مواجهة الجرائم المعلوماتية.

4- دعوة السلطات العراقية الى ايجاد غطاء قانوني يمنح سلطات الضبط الاداري، السلطات اللازمة لحجب المواقع والبرامج التي تؤثر على منظومة الاخلاق والقيم في المجتمع العراقي وتنافي الذوق العام والآداب العامة، والتعامل مع شبكة الانترنت بشكل يخدم مقومات الدولة ويحافظ على حقوق رعاياها.

5- صحيح ان قانون البطاقة الوطنية هو الوحيد في المنظومة القانونية الذي نصّ على توطين البيانات، الا انه جاء خاص ببيانات محددة المدنية فقط دون غيرها، فضلاً عن عدم تضمنه عقوبات على من يستخدم تلك البيانات بطريق غير مشروع، لذلك لابد من اعادة قراءة هذا القانون وتعديله.

المراجع

General Data Protection Regulation, Regulation (EU) . (2016).

CORY, N., & DASCOL, L. (2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost,and How to Address Them.* INFORMATION TECHNOLOGY & INNOVATION FOUNDATION.

Griffiths, C. (2023). *The Latest 2023 Cyber Crime Statistics.* Retrieved 2024, from https://aag-it.com/the-latest-cyber-crime-statistics/

Hill, J. F. (2014). *THE GROWTH OF DATA LOCALIZATION POST-SNOWDEN: ANALYSIS AND RECOMMENDATIONS FOR U.S. POLICYMAKERS AND INDUSTRY LEADERS.* LAWFARE RESEARCH PAPER SERIES, vol 2, no3.

Hong, Y. (2019). *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.

Khalifa, E. (n.d.). *2. Ehab Khalifa, Why would countries think of building national cyber networks? , 2Why_would_countries_think_of_building_National_Cyber_Networks.* Retrieved 2024, from 2. Ehab Khalifa, Why would countries think of building national cyber https://www.academia.edu/24983954

Malcolm , J., & Panday, J. (2018). *THE POLITICAL ECONOMY OF DATA LOCALIZATION.* Journal of Sociopolitical Studies,Issue 11(2).

Selby, J. (2017). *Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?* International Journal of Law and Information Technology, Volume 25, Issue 3.

Shahbaz, A., Funk, A., & Hackl, A. (2020). *22. Adrian Shahbaz, Allie Funk and Andrea Hackl, User Assessing the human rights implications of data localization, Freedom House special report 2020.* Freedom House special.

Swire, P., Kennedy-Mayo, D., & Bagley, D. (2023). *Risks to Cybersecurity from Data Localization, Organized by Techniques,Tactics, and Procedures.* American University School of Public Affairs Research Paper No. 4466479.

Szczepański, M. (2020). *31. Marc Is data the new oil? Competition issues in the digital economy.* European Parliamentary Research Service.

urban, C. (2021). *the cloud of a bloodless war; data localization and the securitization of cyberspace in India.* Vienna, Austria: Central European University Department of international Relations.

Ursic, H., Nurullaev, R., & Cuevas, M. (2018). *SSRN Prouduct & Servies*. (H. o. science, Producer) Retrieved 4 1, 2024, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102890

Wu, E. (2021). *Sovereignty and Data Localization.* Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School.

قاموس ومعجم متعدد المعاني والمجالات. (2000). تاريخ الاسترداد 10 4, 2024، من موقع قاموس ومعجم متعدد المعانيوالمجالات: https://www.almaany.com/

Encyclopedia, data localization .(2021) .Encyclopedia, data localization: https://encyclopedia2.thefreedictionary.com/data+localization. تاريخ الاسترداد 3, 2024، من

Basuroy, T. (2022). *Number of cybercrimes reported across India from 2012 to 2021.* Retrieved 2024, from https://bit.ly/3Ue3E8q.

Millard , C. (1985). *Legal Protection of Computer Programs and Data.* london.

Panday, J., & Malcolm, J. (2018). *The political economy of data localization.* Journal of Sociopolitical Studies, Issue 11(2).

report, I. s. (2022). *digital authoritarianism returning across the globe.*

Sheppard, L., Yayboke, E., & Ramo, C. (2021). *THE SHIFT TOWARD DATA LOCALIZATION.* CSIS international security program.

Swami Vivekananda .(2018) .*DATA LOCALISATION IN A GLOBALISED WORLD DATA LOCALISATION IN A GLOBALISED WORLD An Indian Perspective* .The Dialogue C/O Foundation for Progressive Narrative.

احمد فتحي سرور. (1995). *الشرعية الدستورية وحقوق الانسان في الاجراءات الجنائية ، القاهرة ، دار النهضة العربية ،1995*. القاهرة: دار النهضة العربية.

الشحات ابراهيم محمد منصور. (2011). *الجرائم الالكترونية في الشريعة الإسلامية والقوانين الوضعية* (المجلد 1). الاسكندرية: دار الفكر الجامعي.

جميل عبد الباقي الصغير. (2002). *الإنترنيت والقانون الجنائي ، دار النهضة العربية ، القاهرة ، 2002*. القاهرة: دار النهضة العربية.

حيدر غازي فيصل. (2008). حيدر غازي فيصل ، الحق في الخصوصية وحماية البيانات ، بحث منشور في ، جامعة النهرين ، المجلد 11 ، العدد 21 ، 2008. *مجلة كلية الحقوقن المجلد 11، ع 21*، الصفحات 294-295.

د. ميلودي حبيبي. (2011). *المعجم الموحد لمصطلحات تقانة)تكنولوجيا المعلومات*. المنظمة العربية للتربية والثقافة والعلوم: الدار البيضاء.

رافع خضر صالح . (1993). الحق في الحياة الخاصة وضماناته في مواجهة اسخدامات الكومبيوتر. *رسالة ماجستير*، 65-66. جامعة بغداد- كلية القانون.

سامح محمد عبد الحكم. (2007). *17. سامح محمد عبد الحكم ، جرائم الانترنت الواقعة على الأشخاص في إطار التشريع البحريني ، دار النهضة العربية ، القاهرة ، 2007*. القاهرة: دار النهضة العربية.

سيد محمود. (2023). *حماية البيانات الشخصية الرقيمة وفقاً لاحكام القانون المصري رقم 151 لسنة 2020(حماية البيانات الشخصية المعالجة الكترونياً) بين الواقع والمأمول*. مجلة العلوم القانونية والاقتصادية، ع1.

صبحي المحمصاني . (1979). *اركان حقوق الانسان*. بيروت: دار العلم للملايين.

علي سيد اسماعيل. (2019). *الامن القومي العربي واقعة في ظل التحولات الاقتصادية المعاصرة*. الاسكندرية: دار التعليم الجامعي.

علي احمد عبد الزغبي. (2006). *حق الخصوصية في القانون الجنائي (دراسة مقارنة)* (المجلد 1). لبنان: المؤسسة الحديثة للكتاب.

عمر ، حسبو. (2000). *حماية الحريات في مواجهة نظم المعلومات*. القاهرة: دار النهضة.

ماجد راغب الحلو. (2005). *النظم السياسية والقانون الدستوري*. الاسكندرية: منشأة المعارف.

محمد بن أبي بكر بن عبد القادر الرازي. (1987). *مختار الصحاح ، دار الكتاب الحديث ، ج1، 1987*. دار الكتاب الحديث.

محمد زكي ابو عامر. (1979). *الحماية الجنائية للحريات الشخصية ، الاسكندرية ، منشاة المعارف ، 1979*. الاسكندرية: منشأة المعارف.

محمد سعيد خشبة. (بلا تاريخ). *مقدمة في الحاسبات الالكترونية*. دار الكتب.

محمد محمود المكاوي. (2010). *الجوانب الأخلاقية والاجتماعية للجرائم المعلوماتية* (المجلد 1). مصر: المكتبة العصرية للنشر والتوزيع.

منى الاشقر جبور. (2016). *السيبرانية هاجس العصر*. بيروت: المركز العربي للبحوث القانونية والقضائية.

نشوان بن سعيد الحميري . (1999). *شمس العلوم ودواء كلام العرب من الكلوم*. بيروت: دار الفكر المعاصر.