ISSN: 1999-5601 (Print) 2663-5836 (online)

Lark Journal

Available online at: https://lark.uowasit.edu.iq

*Corresponding author:

Dr. Samer Mohi Abdel Hamza

University: Wasit University

College: College of Law

Email: Smuhhi@uowasit.edi.iq

Keywords:

International Law, International Organizations, cybersecurity, Iraqi cybersecurity

A R T I C L E I N F O

Article history:

Received	11 Apr 2022
Accepted	8 Jun 2022
Available online	1 July 2022

The Iraqi Legislative Policy to Protect National Cyber Security

A study in the light of the principles of public international law

A B S T R U C T

Cybersecurity protection from foreign threats regard a constant challenge for international organizations and that organisations tries to choose a legislative policy that maintains the security of member states on the one hand , and respect for the human rights recognized by international organization's charters with respect to individual freedoms.

The most important is the study of Iraq's position on the adoption of a legislative policy contributing to the protection of Iraqi cybersecurity against the constants dangers to Iraqi's official websites.

We will address the topic in three chapter, in the first chapters we will address the search for the definition of cybersecurity and its different meanings, and then deal in the Second chapter with the Policies adopted by international organizations regarding cybersecurity and their impact on individual freedoms, finally in the third and last chapter We address the existing system of cybersecurity in Iraq and the crucial gaps and suggestions to improve the legislative policy regarding the protection of cybersecurity in Iraq.

DOI: https://doi.org/10.31185/

السياسة التشريعية العراقية لحماية الأمن الوطني السيبراني
دراسة في ضوء احكام القانون الدولي العام

أ.م.د سامر محي عبد الحمزة/كلية القانون/ جامعة واسط

الخلاصة:

تشكل حماية الأمن السيبراني للدولة من التهديدات الخارجية هاجساً يشغل المنظمات الدولية كافة، إذ يتوجب عليها ان تختار سياسة تشريعية تحافظ على أمن الدول الاعضاء فيها من جهة واحترام مبادئ حقوق الانسان التي تقرها مواثيق المنظمات الدولية فيما يتعلق باحترام الحريات الفردية من جهة أخرى.

والأهم من ذلك دراسة موقف العراق من تبني سياسة تشريعية تساهم في حماية الأمن السيبراني العراقي ضد المخاطر التي تتعرض لها المواقع الالكترونية الرسمية بشكل دائم.

وسوف نعالج الموضوع في ثلاثة مباحث، نتناول في المبحث الاول تعريف الأمن السيبراني والدلالات المختلفة له، ثم نتناول في المبحث الثاني السياسات التي تبنتها المنظمات الدولية بخصوص حماية الأمن السيبراني ، وتأثيرها على الحريات الفردية؛ لنصل الى المبحث الثالث والاخير الذي نتناول فيه واقع الأمن السيبراني في العراق واهم الثغرات فيها واقتراحاتنا لتحسين الواقع التشريعي الخاص بحماية الامن السيبراني في العراق.

الكلمات المفتاحية: القانون الدولي العام، المنظمات الدولية، الأمن السيبراني، الأمن السيبراني العراقي.

المقدمة

أهمية البحث

إن الفضاء السيبراني هو مكان تتشابك فيه سيادة الدول، فهو مكان مشترك لا يمكن أن تستقل دولة بذاتها بتنظيمه؛ لذلك فإن بحثنا للسياسة السيبرانية للعراق لا يمكن أن يكون بمعزل عن الدول التي تشاركنا في هذا الفضاء.

وقد تصدت المنظمات الدولية الإقليمية منذ بدايات الألفية الثالثة لموضوع حماية الأمن السيبراني الذي فرضته ظروف التحول الرقمي المتسارع، ومع ذلك نجد أن جامعة الدول العربية هي المنظمة الإقليمية الوحيدة التي لم تعطِ الموضوع حقه، لذلك فأن دول الجامعة تسير كل منها على وفق السياسة الوطنية التي تراها مناسبة، فنجد دولاً قطعت اشواطاً كبيرةً في التأسيس لرؤية تشريعية واضحة للأمن السيبراني مثل الامارات العربية المتحدة والمملكة العربية السعودية ودول لم تتقدم كثيراً كاليمن ولبنان والعراق.

وفي ظل غياب رؤية أقليمية واضحة لجامعة الدول العربية، علينا أن نبحث في الاتجاهات الرئيسة للأمن السيبراني وأيُّهم الافضل تبنيه في العراق، بعد أن نبحث واقع الأمن السيبراني في العراق.

مشكلة البحث

يمثل البحث محاولة اقتراح سياسة تشريعية للأمن السيبراني في العراق في ظل غياب توجه إقليمي عربي واضح، وفي ضوء السياسات التي تتبناها المنظمات الدولية كالاتحاد الأوروبي أو اتحاد الدول المستقلة، إذ يعاني العراق من عدم وجود سياسة واضحة، كما أن الأجهزة التي تعنى بالأمن السيبراني موزعة بين جهاز الأمن الوطني والمخابرات العامة ووزارة الداخلية، ولا توجد وزارة أو هيئة مستقلة للأمن السيبراني.

منهج البحث

سنعتمد في هذا البحث المنهج المقارن منهجاً رئيساً في الدراسة، إذ أن معرفة السياسة التشريعية المثلى لحماية الأمن السيبراني في العراق لا تتم إلا من خلال مقارنتها بمثيلاتها من السياسات للمنظمات الدولية والدول التي سبقتنا في التعامل مع ذلك، كما سنعتمد المنهج التحليلي في دراسة بعض الإشكاليات التي يطرحها الموضوع.

خطة البحث

سوف نقسم هذا البحث على ثلاثة مباحث رئيسة مع خاتمة في نهاية البحث لعرض الاستنتاجات التي توصلنا إليها والتوصيات التي نقترحها، اذ سنتناول في المبحث الأول مفهوم الأمن السيبراني بشقيه العام والخاص، ثم نتناول في المبحث الثاني الاتجاهات الرئيسة للمنظمات الدولية في التعامل مع الأمن السيبراني، ونسلط الضوء في المبحث الثالث على الأمن السيبراني العراقي متناولين فيه واقع الأمن السيبراني ثم الرؤية التشريعية المستقبلية له.

المبحث الاول

مفهوم الأمن السيبراني

إن هناك مفهوماً عاماً للأمن السيبراني كما هو متداول في بعض القوانين والبحوث المختصة يتسم بكثير من الشمول التي تبعده عن مغزاه الحقيقي؛ لذلك نرى أن هذا المفهوم قاصر عن الإحاطة بهذا الموضوع؛ لذلك اقترحنا مفهوم خاص للأمن السيبراني نابع من الطبيعة الخاصة لهذا الأمن.

عليه سوف نقسم هذا المبحث على مطلبين نتناول في المطلب الأول المفهوم العام للأمن السيبراني ونتناول في المطلب الثاني المفهوم الخاص للأمن السيبراني.

المطلب الاول

المعنى العام للأمن السيبراني

أول ما نلاحظه هو انعدام وجود تعريف قانوني للأمن السيبراني تتوافق عليه الدول كافة، والسبب هو إن تقديم تعريف قد يؤدي إلى تقييد سلطة الدولة في التعامل مع المتغيرات التي يفرضها الأمن السيبراني بالإضافة إلى أن المفهوم الوطني للأمن السيبراني في كل دولة لا يزال في طور التشكيل ولم يتخذ طابعاً واضحاً.

والقواميس المتخصصة بالمصطلحات السيبرانية تعد الأمن السيبراني هو إستراتيجية أو سياسة تتبعها الحكومات المختلفة للتعامل مع المخاطر الناشئة عن الفضاء السيبراني(Springer, 2017, p.62).

ولعل التعريف الأقرب هو التعريف الفني الذي طرحته المنظمة الدولية للاتصالات وهي احدى المنظمات المتخصصة التابعة للأمم المتحدة، التي عرفته بأنه" مجموعة *السياسات والأدوات والمعايير التي تستخدم لحماية الفضاء السيبراني من الدخول غير المصرح به، وسوء الاستغلال، واستعادة المعلومات الإلكترونية، ونظم الاتصالات والمعلومات التي تحتويها، وذلك لضمان استمرار عمل نظم المعلومات، وتعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية الأشخاص والمستخدمين من المخاطر في الفضاء السيبراني*" (الاتحاد الدولي للاتصالات،2008، ص8).

ووفقاً لهذا المعنى فالأمن السيبراني هو عبارة عن سياسة متكاملة للتعامل مع مجمل المشاكل التي يثيرها الفضاء الرقمي ولا يقتصر على المشاكل ذات الطابع الأمني كما لا يقتصر مفهومه على الجوانب القانونية والإدارية وإنما يدخل فيه الجوانب الفنية المتعلقة بأمن شبكات الاتصال التي تقع على عاتق المهندسين المختصين في الشركات المعنية بتجهيز خدمة الإنترنت.

وتعتمد المنظمة الدولية على عدد من المؤشرات أو المعايير لقياس مستوى الأمن السيبراني في الدولة، وهذه المعايير ترتكز على خمسة محاور:

المحور التشريعي يقيس وجود بيئة تشريعية لمواجهة التحديات السيبرانية. يفترض توفر مجموعة من التشريعات التي تنظم الفضاء السيبراني، والمحور الفني الذي يتعلق بوجود هيئات الاستجابة السريعة للحوادث السيبرانية، والمحور التنظيمي الذي يتعلق برسم استراتيجية الأمن السيبراني، والمحور العملياتي المتعلق ببناء القدرات المحلية والتوعية بالأمن السيبراني، والمحور التعاوني المتعلق بالشركات مع القطاع

الخاص ومع المنظمات الدولية للتعاون في جهود تحقيق الأمن السيبراني (International Telecommunication Union, 2020,p.3) .

وهذا المعنى العام لا يقدم فائدة كبيرة للمختصين بالموضوع بقدر ما يكون سبباً في تشتيت جهات المسؤولية عن الأمن الوطني السيبراني، فالأخذ بالتعريف السابق كما هو يفضي الى نتائج غير مقبولة، لأنه يجعل الأمن السيبراني شاملاً لكل ما يتعلق بالفضاء السيبراني، فمن غير المنطقي أن نجعل صيانة شبكات الانترنيت أو حماية مواقع التواصل الاجتماعي للفنانين على سبيل المثال جزءً من الأمن السيبراني للدولة.

لذلك فالمفهوم العام يبقى صالحاً لمعرفة الواقع السيبراني لدولة ما في مدة محددة، فهو يصلح أن يكون مؤشراً للواقع السيبراني، أما الأمن السيبراني فلا يمكن أن يكون بهذا الاتساع ؛ لذا يجب أن نبحث في المعنى الخاص للأمن السيبراني.

المطلب الثاني

المعنى الخاص للأمن السيبراني

في اعتقادنا أن الأمن السيبراني يبقى فرعاً من فروع الأمن الوطني، أو هو بعد من أبعاد الامن القومي للدولة، إذ أن أمن الدولة وحمايته يبقى واحداً مع اختلاف في نطاقه، والفضاء السيبراني يبقى بيئة مستحدثة نشأت نتيجة توغل الانترنت في الحياة العامة والخاصة بشكل أصبحت بعض النشاطات فيه تمثل تهديداً كبيراً للأمن الوطني للدولة، فيبقى العنصر الأمني هو الاساس في أي تشريع سيبراني.

وأفضل تعريف للأمن السيبراني ممكن ان نستقيه من التعريف الذي تبناه القانون المصري لعام ٢٠١٨ للأمن القومي، إذ عرفه بأنه "كل ما يتصل باستقلال واستقرار وامن الوطن ووحدة وسلامة أراضيه" (قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة ٢٠١٨ المصري، المادة 1) وقريب منه القانون الفيتنامي الذي عرَّف الأمن السيبراني بأنه "ضمان ان تكون كافة الافعال في الانترنيت لا تضر بالأمن الوطني للدولة" (Socialist Republic of Vietnam, 2018, p.1).

لذلك يمكن القول بضرورة استبعاد ما يأتي من مفهوم الامن السيبراني:

1. مكافحة الجريمة الإلكترونية (Cybercrimes policy): هي السياسة الجنائية التي تتبعها الدولة في مكافحة الجرائم الإلكترونية، وغالباً ما يتم صياغتها إمّا عن طريق إتباع القواعد العامة في القوانين

الجزائية وتطبيقها على الجرائم السيبرانية أو بتشريع قوانين جديدة تكفل لمكافحة الجريمة الإلكترونية (Kittichaisaree, 2017, p.263).

2. أمن الشبكات (Networks Security): لا يمكن أن يشمل الأمن السيبراني حماية البنى التحتية من أجهزة حواسيب وبنايات أو حسابات شخصية أو شركات مزودي الخدمة في الدولة، إذ أن أمن الشبكات وإن كان يدخل في المفهوم العام للأمن السيبراني لكن يجب استبعاده لإمكانية تركه للجهات الفنية المختصة مثل وزارة الاتصالات(Graham and others, 2011, p.25) .

3. حماية النظام العام والآداب العامة في الفضاء السيبراني، الذي تتولاه وزارة الداخلية والجهات التابعة لها من غير أن يكون من مسؤولية الجهات الأمنية.

وغالباً ما تناط مسؤولية حماية الأمن السيبراني الى هيئة مستقلة قد تكون وزارة أو مجلس أو اتحاد، وهذا يختلف من دولة إلى اخرى، فهي المجلس الوطني للأمن السيبراني في الأردن (قانون الأمن السيبراني الاردني، 2019، ص5144) أو المجلس الأعلى للأمن السيبراني في مصر (مجلس الوزراء المصري، 2014، قرار 2259) أو الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية (المملكة العربية السعودية، الامر الملكي رقم 6801).

المبحث الثاني

السياسات التشريعية الحالية للمنظمات الدولية

إن تحديد سياسة معينة للأمن السيبراني يتضمن بعض الآليات التي لها تأثير على الحريات الفردية؛ لذلك عند صياغة أي رؤية تشريعية يجب ابتداءً الموازنة بين حماية الأمن السيبراني من جهة وحماية الحريات الفردية من جهة أخرى.

وتدخّل الأجهزة الأمنية يضيق في الدول ذات النظم الديمقراطية ويتوسع في الدول ذات النظم الشمولية، ولعل أهم اتجاهين تبنتهما المنظمات الدولية الإقليمية بهذا الشأن هما حرية الفضاء الإلكتروني الذي يجعل الأساس هو احترام الحريات الفردية والتدخل لحماية أمن الدولة السيبراني هو الاستثناء، وبين سياسة التحكم بالفضاء السيبراني التي تغلِّب موضوع حماية أمن الدولة على الحريات الفردية وتجعل مسالة سيادة الدولة على هذا الفضاء محور سياستها السيبرانية.

عليه سوف نتناول هذين الاتجاهين في مطلبين، يتناول المطلب الأول سياسة الفضاء السيبراني المفتوح ونتناول في المطلب الثاني سياسة التحكم بالفضاء السيبراني.

المطلب الاول

سياسة الفضاء السيبراني المفتوح

ويمثله حالياً الاتحاد الأوروبي والولايات المتحدة الامريكية.

وقد نشأت في الأصل في الولايات المتحدة مع نشوء الانترنت وتقوم على الحرية وعدم اخضاع الانترنيت لأي سلطة، بل أن نشوء الفضاء كان للهروب من رقابة الدولة، إذ سمي بأنه الفضاء الرابع والفكرة الأساسية هو فضاء بلا حدود يضمن التدفق الحر للمعلومات. وظهر إعلان حرية الانترنت عام 1998 (Thierer and Crews, 2003, p.22).

وهذه السياسة تقوم على حيادية الفضاء الرقمي (Neutrality) وهي تضع حقوق الإنسان وحرياته ضمن أولويات الدولة، والاستثناء هو تقييدها لمقتضيات الأمن العامة، وهي وإن كانت تعطي الأولوية للأمن إلا انها تعطي منزلة مساوية له هي احترام حرية التعبير والخصوصية، فالأمن لا يمكن أن يكون مبرراً لتقييد الحرية إلا في حالات خاصة(World Bank, 2017, p.167).

وتقوم هذه السياسة على ثلاثة مبادئ:

1. مبدأ الضرورة (Necessity) أي أن الأصل هو احترام الخصوصية ، وحماية الأمن الوطني هي الضرورة التي تبيح تدخل الدولة في رقابة نشاطات ؛ لذلك تم إبطال عدد من قوانين الاتحاد الاوروبي ؛ لأنها جاءت خالية من الضرورة.

فعلى سبيل المثال ألغت المحكمة الأوروبية لحقوق الإنسان الامر التشريعي الصادر عن الاتحاد الاوروبي رقم (٢٤) لسنة ٢٠٠٦ والذي ألزم الشركات بضرورة الاحتفاظ بالمراسلات الإلكترونية للأفراد لمدة ستة أشهر والسماح للجهات الأمنية بالاطلاع عليها، وقد جاء في قرار المحكمة أن الامر التشريعي يتضمن إمكانية الوصول لأسماء وعناوين ومراسلات وتنقلات المستخدمين الإلكترونية، وهذه البيانات جزء من الخصوصية التي يجب ضمانها؛ لذلك فإن الأمر التشريعي يمثل تجاوزاً كبيراً على حقوق الانسان الأساسية المتمثلة بالحق في الخصوصية والحق في حماية البيانات الشخصية(Court of Justice, 2014).

2. مبدأ تحديد المدة (temporary measures) أي أن تنفيذ إجراءات رقابة حسابات الافراد تسري لمدد معينة وتكون بحاجة للتجديد السنوي مع ضرورة موافقة السلطة التشريعية عند التجديد، وهي حالات الطوارئ التي تنظمها الدساتير الوطنية، وهذا الشرط ينطبق على جميع حالات الدخول غير المصرح به من قبل أجهزة الدولة الأمنية لحسابات الأفراد من قبل الجهات الامنية لمنع الجرائم التي تمس أمن الدولة (Loideain, 2015, p.55).

ولعل أكبر مثل على ذلك هو قانون مكافحة الإرهاب الأمريكي المعروف بإسم (patriot Act) بعد تفجيرات برجي التجارة العالمي في ١١ ايلول ٢٠٠١، إذ أن أغلب نصوصه انتهت عام ٢٠٠٤، لكن تم تجديد البعض منها لسنة أو سنتين، وهو حالياً قد أُوقف تنفيذه. (Bendix and Quirk, 2015, p.5).

3. مبدأ الرقابة القضائية (judicial review) ويعني أن جميع أعمال الحكومة تخضع لرقابة القضاء، وتدخّل القضاء يكون بشكلين، سابق ولاحق، السابق يقتضي الحصول على أمر قضائي للحصول على المعلومات الشخصية، واللاحق يعني إمكانية الطعن بإجراءات الأجهزة الأمنية أمام محكمة مختصة (European Union Agency for Fundamental Rights, 2015, p.61).

وبذلك نلاحظ أن هذا الاتجاه أحاط سرية المعلومات الشخصية وحق الخصوصية بسياج من الضمانات يصعب معها على الأجهزة الأمنية أن تستغل سلطتها أو تسئ استخدامها.

المطلب الثاني

سياسة التحكم بالفضاء السيبراني

ويمثل هذه السياسة اتحاد الدول المستقلة (الذي يضم الدول التي استقلت بعد تفكك الاتحاد السوفيتي وعلى رأسها روسيا الاتحادية)، كما سارت على هذا الطريق جمهورية الصين التي يتقارب نظامها السياسي مع النظام الروسي من حيث تبني نظام الحزب الواحد وتقييد الحريات الفردية.

وتقوم هذه السياسة على إخضاع الفضاء السيبراني لسيادة الدولة، اذ هو في نظرهم امتداد للتلفاز والبث الراديوي، لذلك تحاول تلك الدول إبراز فكرة سيادة الدولة على الفضاء السيبراني وترى أن لكل دول الحق في تنظيم فضائها الإلكتروني.

ويسود في هذا الاتجاه تعظيم المخاطر الأمنية وإعطاء التهديدات الأمنية اهتمام أكبر بكثير من حماية الحريات الفردية، إذ تبنت دول الاتحاد ما يسمى بمبدأ (أمن المعلومات) الذي صاغته روسيا الاتحادية مع بداية عام ٢٠٠٠ ويعني أن حماية الأمن الوطني هو الأولوية القصوى عند تنظيم الفضاء السيبراني (Hakala and Melnychuk, 2021, p.14).

وهذا الاتجاه يخول الجهات الأمنية سلطات شبه مطلقة في التعامل مع البيانات الخاصة للأفراد من غير حاجة لاستحصال أمر قضائي، كما لا توجد جهة رقابية أعلى من تلك الجهات الأمنية من الممكن أن تراقب عملها وتمنع استغلالها للسلطات الواسعة الممنوحة لها.

ودول الاتحاد تبنت أغلبها النظام الروسي المسمى (SORM ||) وهو نظام مراقبة النشاطات الذي تم المصادقة عليه في روسيا الاتحادية وأصبح نافذا اعتباراً من عام ٢٠٠٠، ويرتكز على إلزام جميع مزودي الانترنيت بتثبيته في برامجهم، وهو يقوم بتسجيل النشاطات على الانترنت كافة مع عناوين المستخدمين ووقت النشاط (http://www.libertarium.ru/libertarium/37988/).

ويقوم هذا الاتجاه على ثلاثة مبادئ:

1. مبدأ التوطين (data localisation): وهذا المبدأ يتعلق بعدم السماح بمعالجة البيانات التي تخص الدولة ورعاياها في مزود خدمة يقع خارج حدود الدولة، وهي تفرض على شركات مزودي خدمة الانترنت وكذلك شركات التواصل الاجتماعي مثل الفيسبوك والواتس اب وشركة غوغل أن يتم تخزين جميع تلك المعلومات في ذاكرة سحابية ضمن اقليم الدولة ذاتها (Russian Federation, 2006, Art.12).
2. مبدأ الرقابة(surveillance): ويعني أن الأجهزة الأمنية في الدولة تستطيع في أي وقت الدخول للبيانات الشخصية لمستخدمي الانترنت، كما أن شركات خدمة الانترنت ملزمة بالاحتفاظ بمراسلات مستخدمي الانترنت لمدة لا تقل عن ٦ أشهر وتمكين الأجهزة الأمنية من الاطلاع عليها بأي وقت.

وتتمتع أجهزة الامن الروسية والصينية بصلاحية الدخول على البيانات الشخصية للأفراد من غير حاجة لاستصدار أمر قضائي ومن غير أن تخضع لرقابة أي سلطة أعلى منها في هذا الشأن، إذ أن الخصوصية ليست محل اعتبار أمام حماية الامن العام (Russian Federation, Art.6).

3. مبدأ الفلترة (Censorship): وهو حجب المواقع الإلكترونية والبرامج جزئياً أو كلياً إذا رأت ذلك ضرورة لحماية الأمن الوطني، وقد يصل الامر الى عزل الدولة بالكامل عن الشبكة العالمية، وهو المشروع الذي تعمل عليه روسيا الاتحادية حالياً.

والفلترة تتم ايضا من غير اشتراط موافقة جهة معينة، بل هي سلطة تقديرية لثلاث جهات هي الجهات الأمنية، والمدعي العام، والهيئة الفدرالية المشرفة على الاتصالات وتكنولوجيا المعلومات ووسائل الإعلام العامة (Gaydareva, 2020, p.264).

وتطبيق هذا النظام لا يخلو من اثار سلبية على الحريات الاساسية، ولعل اخطرها هو تقييد حرية التعبير ومنع انتقاد الدولة وأدائها بما يؤدي الى تفرد الحكومة بالقرار طالما كان ما تقوم به يبقى بعيداً عن الرقابة الشعبية، وهذه السياسة تثير الشكوك عن امكانية تبني هذا النظام في الدول حديثة العهد بالديمقراطية مثل العراق.

كما أن تطبيق هذه السياسة في الأمن السيبراني جعلت روسيا محلاً للانتقاد من الهيئات الدولية المعنية بحقوق الانسان ؛ لأنها تتناقض مع العديد من الحقوق والحريات المقررة بالمواثيق الدولية مثل الحق في التعبير عن الراي والحق في الخصوصية، وقد سبق أن بين المفوض الخاص لمجلس حقوق الانسان التابع للأمم المتحدة أن التشريعات التي تتبناها روسيا في هذا الشأن تمثل تقييداً غير ضروري للحريات الفردية وممكن ان تستخدم لملاحقة المعارضين للحكومة.(United Nations Human Rights, 2016, p. 4).

وتشير تقارير المنظمات غير الحكومية الى أن روسيا الاتحادية والدول الاعضاء في رابطة الدول المستقلة قامت بالفعل باستخدام هذه السياسة بملاحقة المعارضين وإغلاق العشرات من الواقع الالكترونية التي تنتقد أداء الحكومة أو تتبنى افكاراً مخالفة لسياستها.(Amnesty International, 2014, p.20).

المبحث الثالث

الامن السيبراني العراقي

إن تقديم مقترحات لتعزيز الأمن السيبراني العراقي لا يمكن القيام به قبل معرفة طبيعة النظام الحالي والاستراتيجية المتبعة للتعامل مع الموضوع.

عليه سوف نقسم هذا المبحث الى مطلبين، نتناول في المطلب الأول واقع التنظيم القانوني للأمن السيبراني العراقي، لكي نتبين النظام الحالي له والنواقص التي تعتريه، ثم نتناول في المطلب الثاني الرؤية التشريعية المستقبلية للأمن السيبراني العراقي.

المطلب الاول

واقع التنظيم القانوني للأمن السيبراني العراقي

شهد العراق تحولاً كبيراً في التعامل مع وسائل الأعلام بما فيها الانترنت تمثلت في سياسة الانفتاح الكلي على الفضاء السيبراني، ويمكن القول ان هذه السياسة دخلت العراق مع دخول القوات الامريكية للعراق ٢٠٠٣، إذ شهد العراق انفتاحاً واسعاً على البيئة السيبرانية التي كانت مغلقة في ظل النظام السابق.

وقد كانت السياسة التي صاغتها سلطة الائتلاف المؤقتة المنحلة في التعامل مع الفضاء الإلكتروني متأثرة كثيراً بسياسة الفضاء المفتوح التي تتبناها الولايات المتحدة، إذ اتخذت هذا السياسة محورين:

الأول: حرية وسائل الاعلام وفتح الفضاء الالكتروني ومنح الافراد الحرية الكاملة في الوصول الى محتوياته او النشر من خلاله ومعاملته معاملة مساوية لوسائل الاعلام الأخرى، وقد اتخذت هذه السياسة بعداً تشريعياً من خلال الغاء وزارة الاعلام وانشاء المفوضية العليا للاتصالات والاعلام في اذار ٢٠٠٤ (أمر سلطة الائتلاف المؤقتة (المنحلة) رقم ٦٥، 2004، ص2).

الثاني: تقليل الرقابة الأمنية على وسائل الاعلام بما فيها الانترنت عن طريق الغاء الاجهزة والمؤسسات الأمنية التي كان يستخدمها النظام السابق لإحكام سيطرته على الدولة، وتم الاستعاضة عنها بإنشاء جهاز أمني موحد هو اللجنة الوزارية للأمن القومي في نيسان ٢٠٠٤.(أمر سلطة الائتلاف المؤقتة (المنحلة) رقم 68، 2004، ص3).

ومنذ ذلك الحين لم يحدث تغيير رئيس في هذه السياسة، بل أن قرارات سلطة الائتلاف المؤقتة المنحلة بشأن القانونين السابقين لا زالت نافذة على الرغم من مرور ما يقارب العقدين منذُ الغاء سلطة الائتلاف المؤقتة.

والعراق ليس الدولة العربية الوحيدة التي لا تراجع او تحدث تشريعاتها السيبرانية، بل أن وعدم تحديث السياسات التشريعية السيبرانية هي سمة غالبة للدول العربية التي ما زالت تتجاهل أخطار الواقع السيبراني كما أشار الى ذلك تقرير المنظمة العربية للاتصالات والمعلومات عام ٢٠٢١.(المنظمة العربية لتكنولوجيا الاتصالات والمعلومات، 2021، ص16).

وحالياً فان تقويم الأمن السيبراني في العراق وفقاً لتقرير الاتحاد الدولي للاتصالات هو ٢٠ من مئة درجة، ويحتل الموقع ١٢٩ من أصل ١٨٢، إذ يقع في ترتيب الدول الأضعف في الأمن السيبراني تتفوق

عليه غالبية الدول العربية حتى الدول الضعيفة في القدرات المالية والفنية مثل السودان ولبنان وسوريا وفلسطين.(International Telecommunication Union, 2020,p.72).

مع ملاحظة أن العراق من أكثر الدول التي تتعرض للهجمات الالكترونية، وغالباً ما تُعطل الصفحات الرسمية الخاصة بالوزارات الامنية مثل وزارة الداخلية ومستشارية الأمن الوطني وجهاز مكافحة الإرهاب، ولعل أخطرها كان في ٢٥ تشرين الثاني ٢٠١٩ عندما تم اختراق الموقع الرسمي لجهاز مكافحة الإرهاب والاعلان عن انقلاب ضد الحكومة استجابةً لدعوة المتظاهرين، الا ان جهاز مكافحة الإرهاب أعلن في موقعه الالكتروني الرسمي لاحقاً عن تعرض الموقع للاختراق وان ما نشر فيه ليس صحيحاً. (https://www.alkawthartv.ir/news/219576/)

والخلل الكبير الذي يواجه تنظيم الفضاء السيبراني يتمثل بعدم تطوير سياسة واضحة أو انشاء هيئات تتولى مواجهة التحديات الامنية التي يفرضها الفضاء السيبراني، ويمكن بيان نواقص السياسة الحالية بما يأتي:

1. عدم وجود قانون ينظم الأمن السيبراني

إذ لا توجد قوانين تهتم بالأمن الوطني السيبراني، والدولة العراقية تفتقر لوجود مجالس للأمن السيبراني او أي هيئات مستقلة أخرى ممولة بشكل كاف تتولى هذه المهمة.

ويكفي هنا ان نشير إلى المخاض العسير الذي يمر به قانون الجرائم الالكترونية الذي تم مناقشته في مجلس النواب منذ عام 2011، ولا زال مشروعاً مطروحاً في مجلس النواب منذُ أكثر من عشر سنوات ولم يرَ النور حتى هذه اللحظة بسبب سوء الصياغة والمبالغة في العقوبات التي وردت فيه. (تقرير هيومن رايتس ووتش،2012، ص3).

2. عدم وجود هيئة مختصة بالأمن السيبراني

حالياً لا توجد هيئة مستقلة للأمن السيبراني على الرغم من ذلك نلاحظ أن العراق قد حاول أن يساير بعض الدول في موضوع الامن السيبراني فأنشأ هيئة وحيدة للأمن السيبراني هي (فريق الاستجابة السريعة للأحداث السيبرانية)، وهي هيئة تابعة لمستشارية الامن الوطني (التي هي ذاتها تفتقر لقانون ينظمها لها وانما انبثقت عن اللجنة الوزارية للأمن القومي).

والفريق ما زال في بدايات تكوينه، كما أن موقعه الإلكتروني يتعرض للاختراق أكثر من مرة، وتتهمه بعض وسائل الاعلام بالفساد الاداري وأن أعضاءه يعملون في مكاتب خاصة تتقاطع مع عملهم في هذا الفريق.(Http://skynews/middleeast/).

وقد حاولت الحكومة العراقية تطوير عمله بأن طلبت رسمياً من حلف الناتو تدريب اعضاء الفريق على منذ عام ٢٠١٦.(https://www.nato.int/cps/ua/natohq/news_139179/).

الا أن إمكانيات الفريق تبقى متواضعة قياساً بحجم التحديات التي يفترض به مجابهتها.

وقد أصدر فريق الاستجابة السريعة للأحداث السيبرانية ما أسماه (إستراتيجية الأمن السيبراني العراقي) في ١١ صفحة تضمنت ما يفترض أنه يمثل جوهر سياسة الدولة المتعلقة بحماية الامن السيبراني، مع ملاحظة أن فريق الاستجابة السريعة لم ينشرها في موقعه وإنما الورقة متاحة فقط على موقع الاتحاد الدولي وللاتصالات ضمن قسم تقارير الدول.(https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pd).

وكأن الفريق اراد منها فقط إظهار رسالة للعالم مفادها وجود جهاز أمن سيبراني في العراق من غير اهتمام حقيقي بالموضوع.

والاستراتيجية جاءت مخيبة كثيراً إذ لم تتضمن طبيعة المشاكل وتحديد المهام التي يجب انجازها لتعزيز الامن السيبراني، اذ ورد فيها عبارات عامة تشير الى التمني والرغبة وليس سياسة جادة لمواجهة المشكلة، فقد ورد فيها ما يأتي:

1. ضرورة انشاء قوانين سيبرانية جديدة مثل قانون أمن الاتصالات.
2. ضرورة انشاء منصة مركزية للعمل السيبراني.
3. العمل على سد الفجوة الامنية السيبرانية.

كما تضمنت الإستراتيجية مدد زمنية تتراوح بين عام وخمسة اعوام لإنجاز هذه المهام.

لكن الاستراتيجية لم تبين من هي الهيئة المكلفة بإنجاز كل هذه المهمات الصعبة في ظل عدم وجود قانون للأمن السيبراني أو هيئة مستقلة له أو حتى بنية تحتية لهذا المشروع.

وكيف يمكن إنشاء قوانين سيبرانية في وقت لم تتم المصادقة على قانون جرائم المعلوماتية المطروح على مجلس النواب منذ أكثر من ١٠ سنين؟

لذا يمكن القول إن هذه الإستراتيجية هي رؤية غير واقعية ولا يمكن الركون اليها لتحقيق الأمن السيبراني العراقي وهي إن دلت على شيء فتدل على انعدام رؤية واضحة للأمن السيبراني.

المطلب الثاني

الرؤية التشريعية المستقبلية للأمن السيبراني العراقي

إن القصور في واقع الأمن السيبراني ليس بالأمر الخفي، بل هو ظاهر حتى للجهات الدولية، وقد بدا ذلك واضحاً من تعقيب الامين العام للاتحاد الدولي للاتصالات أثناء زيارته للعراق في ١٥ كانون الاول عام ٢٠١٩ للمشاركة بافتتاح مشروع اتصالات، فبعد أن استمع لشرح وزير الاتصالات العراقي عن تطوير القدرات الفنية العراقية أشار الأمين العام الى أن العراق بحاجة كبيرة الى الاستثمار في ميدان تكنولوجيا المعلومات (https://www.itu.int/hup/2020/5/).

والواقع إن تبني سياسة فعالة للأمن السيبراني ترتكز على محور واحد اساسي وليس عدة محاور كما ترسمه معايير الاتحاد الدولي للاتصالات، هذا المحور هو المحور التشريعي المتعلق بتشريع القوانين المتعلقة ببناء القدرات السيبرانية للدولة العراقية، فلا يمكن الحديث عن هيئات تعنى بالأمن السيبراني في ظل عدم وجود قانون يتعلق بإنشاء هيئة للأمن السيبراني لديها استقلال مالي ترتبط برئاسة الوزراء بشكل مباشر.

ان إقرار هذا القانون يمكن ان يحل الكثير من إشكالات الامن السيبراني كافة من خلال انشاء مجلس للأمن السيبراني وتزويده بفريق متخصص من وزارة العلوم والتكنولوجيا ووزارة الاتصالات ومراكز الحاسوب في الجامعات العراقية، وتخصيص مبالغ مالية مناسبة من الموازنة العامة لتطوير الفريق أدارياً والتعاقد مع الشركات الأجنبية لإنشاء وحدات أمنية متخصصة بالمخاطر السيبرانية، وهذا ما سارت عليه دول: الامارات العربية المتحدة، وقطر، ومصر إذ حصلت كل من هذه الدول على ما يزيد على ٩٥ نقطة من مؤشر الأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات (International Telecommunication Union, 2020,p.71).

إن السياسة الحالية والتي تعتمد الفضاء المفتوح هي الأنسب حاليا للعراق إذا تم تطويرها وإمدادها بالقدرات المادية والبشرية لتقترب من النموذج الأوروبي، أما سياسة التحكم بالفضاء السيبراني فلا يمكن تبنيه في العراق للأسباب الأتية:

1. إن إعطاء السلطة التنفيذية قدر كبير من الصلاحيات في الفضاء الالكتروني من شأنه ان يكون عرضة لإساءة الاستخدام من قبل هذه السلطة في تقييد الحريات الفردية وملاحقة المعارضين ومحاكمة منتقدي السلطة بشكل عام، فإذا أخذنا بالحسبان أن العراق من الدول التي تصنف بالأكثر

فساداً في مؤشر منظمة الشفافية العالمية، فإن منح هذه السلطات سوف يحبط جهود الاصلاح والكشف عن الفساد الاداري.

لذلك لا عجب أن يتعرض مشروع قانون الجرائم الإلكترونية لانتقادات كثيرة من جانب المنظمات الدولية المعنية بحقوق الانسان وكذلك الى اعتراض الكثير من النواب عليه أدت الى عدم التصويت عليه ورفعه من جدول الأعمال بسبب الخشية من استخدامه في ملاحقة أصحاب الراي.

2. إن النظام السياسي العراقي هو نظام ديمقراطي يقوم على الانتخاب والتعددية الحزبية وتداول السلطة، واحد مرتكزات هذا النظام هو حرية التعبير، لذلك لا يتلاءم تركيز سلطات السيطرة على الفضاء السيبراني لدى السلطة التنفيذية في وقت اصبح الفضاء السيبراني انعكاساً حقيقياً للنظام الديمقراطي الذي يكون فيه التعبير السلمي عن الرأي أساس هذا النظام وسبب استمراره.

الخاتمة

في ختام هذا البحث يقتضي ان ندرج عدداً من الاستنتاجات التي توصلنا إليها وعدد من التوصيات التي نقترحها، وكما يأتي:

اولاً: الاستنتاجات

1 . إن الأمن السيبراني يعد جزءً مهماً من أمن الدولة وأصبح أكبر تحد تواجهه الحكومات الوطنية، وهذا الامر يتخذ أهمية أكبر في العراق، اذ تتعرض المواقع الالكترونية الرسمية بما فيها مواقع الأجهزة الأمنية للاختراق المستمر.

2 . إن السياسات التي تبنتها المنظمات الدولية الإقليمية عند وضع التشريعات الخاصة بالفضاء السيبراني تأثرت كثيراً بفلسفة النظام السياسي الذي تتبناه دول المنظمة، لذلك يجب قبل تبني أي سياسة ان ننظر في مدى ملائمتها للنظام السياسي في الدولة، فآثارها متعددة على الحريات الفردية، لذلك لا يمكن القول بوجود سياسة سيبرانية موحدة في العالم يمكن للعراق ان يتبعها.

3 . يعد العراق من الدول الضعيفة في مجال الأمن السيبراني ولا يزال في بداية تعامله مع هذه المسالة، والفريق الذي يتولى مسؤولية الامن السيبراني العراقي قليل العدد مع ضعف في الامكانات وغموض في الصلاحيات ولا يمكن الاكتفاء به في مواجهة المخاطر المتزايدة على الأمن الوطني من قبل القراصنة المحترفين وأجهزة المخابرات المتخصصة في الحوادث السيبرانية.

ثانياً: التوصيات

1. العمل على انشاء مجلس للأمن السيبراني كما هو موجود حالياً في دول: جمهورية مصر، والمملكة العربية السعودية، والاردن وغيرها من الدول بما يضمن ان يضم في عضويته ممثلين عن الجهات الامنية كافة مثل مستشارية الامن الوطني وجهاز المخابرات العامة ووزارة الداخلية لتوحيد سياسات المجلس بخصوص التهديدات الأمنية، ولضمان ان يكون تنفيذ سياسات المجلس شاملاً للأجهزة الأمنية كافة.
2. اكمال قراءة واصدار التشريعات السيبرانية المطروحة امام مجلس النواب العراقي وانشاء مجموعة متكاملة للتشريعات الخاصة بالفضاء السيبراني، والاهم من ذلك هو تفعيل عمل لجان مجلس النواب المتعلقة بالأمن الوطني بأن يتم تشكيل لجنة دائمة للأمن السيبراني في المجلس تتولى مهمة اقتراح التشريعات السيبرانية ومتابعة إصدارها.
3. تخصيص مبالغة مناسبة من الايرادات العامة للدولة العراقية لحماية الأمن السيبراني توازي ما يتم انفاقها عليه في الدول العربية المجاورة، اذ لا يمكن التعامل مع الأمن السيبراني بقلة من الاهتمام كما يحصل حالياً، مع ما يتعرض له العراق ومؤسساته الأمنية من تهديدات سيبرانية قد تهدد الأمن الوطني من خلال استمرار اختراق المواقع الالكترونية الرسمية وإظهار مؤسسات الدولة الأمنية بمظهر العاجز عن الدفاع عن أمنه.

مصادر البحث

اولا : المصادر العربية

أ. الكتب

1. الاتحاد الدولي للاتصالات، السلسلة X، شبكات البيانات والاتصالات بين الانظمة المفتوحة ومسائل الامن، لمحة عامة عن الامن السيبراني، التوصية ١٢٠٥، ٢٠٠٨.
2. المنظمة العربية لتكنولوجيا الاتصالات والمعلومات، الرؤية العربية للأمن السيبراني: الواقع- التحديات- الفرص، جامعة الدول العربية، تونس، ٢٠٢١.
3. هيومن رايتس ووتش، قانون جرائم المعلوماتية العراقية، قانون سيئ الصياغة وعقوبات غاشمة تخرق الحق في إجراءات التقاضي السليمة وتنتهك حرية التعبير، تموز، ٢٠١٢.

ب. المواقع الالكترونية

1. http://www.libertarium.ru/libertarium/37988/
2. /https://www.alkawthartv.ir/news/219576
3. Http://skynews/middleeast/
4. /https://www.nato.int/cps/ua/natohq/news_139179
5. https://www.itu.int/hup/2020/5/
6. https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pd

ت. القوانين والانظمة

1. الامر الملكي رقم ٦٨٠١ في ١١ -٢- ١٤٣٩هجري، تنظيم الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية.
2. امر سلطة الائتلاف المؤقتة (المنحلة) رقم ٦٥ لعام ٢٠٠٤، المفوضية العليا للاتصالات والاعلام، ٢٠ اذار ٢٠٠٤.
3. امر سلطة الائتلاف المؤقتة (المنحلة) رقم ٦٨ لعام ٢٠٠٤، اللجنة الوزارية للأمن القومي، ٤ نيسان ٢٠٠٤.
4. قانون رقم (16) لسنة 2019 قانون الامن السيبراني، الأردن، الجريدة الرسمية 2019.
5. قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة ٢٠١٨ المصري. منشور في الجريدة الرسمية، العدد (٣٢) في ١٤ اغسطس عام 2018.
6. قرار مجلس الوزراء المصري رقم ٢٢٥٩ لعام ٢٠١٤ بإنشاء المجلس الاعلى للأمن السيبراني.

ثانيا المصادر الاجنبية

A. Books, reports, publications

1. Adam Thierer and Clyde Wayne Crews Jr.(editors), Who rules the net?: Internet governance and jurisdiction, the Cato Institute, USA, 2003.
2. Amnesty International, Violations of right to freedom of expression, Association, and Assembly in Russia, Amnesty International October 2014, EUR 46/048/2014.

3. Encyclopaedia of cyber warfare, Paul J. Springer, (editor), ABC-CLIO, LLC, USA, 2017.
4. European Union Agency for Fundamental Rights, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Mapping Member States' legal frameworks, Luxembourg, 2015.
5. Human Rights Watch, Iraq's Cybercrime Law, Poorly Drafted Law and Brutal Punishments that Violate Due Process and Freedom of Expression, July .2012. .(In Arabic).
6. International Telecommunication Union, Global Cybersecurity Index 2020 Measuring commitment to cybersecurity, IT Publications, 2020.
7. International Telecommunication Union, Series X, Data networks and communications between open systems and security issues, an overview of cybersecurity, Recommendation 1205, 2008.(In Arabic).
8. James Graham, Richard Howard, Ryan Olson(edit), Cyber Security Essentials, Taylor & Francis Group, New York, 2011.
9. Janne Hakala, Jazlyn Melnychuk, Russia's strategy in cyberspace, NATO Cooperative Cyber Defence COE, June 2021.
10. Kriangsak Kittichaisaree, Public International Law of Cyberspace, Springer International Publishing Switzerland, 2017.
11. The Arab Organization for Communications and Information Technology, The Arab Vision for Cyber Security: Reality - Challenges - Opportunities, League of Arab States, Tunisia, .2021. .(In Arabic).
12. United nations Human rights, Office of High commissioner, Mandates of special Rapporteur on the promotion and protection of the right of freedom of opinion and expression, 28 July 2016, OL.RUS.7/2016.
13. World Bank and United Nations. 2017. Combatting Cybercrime: Tools and Capacity Building for Emerging Economies, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO.
14.

B. Journals

1. Nora Ni Loideain, EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era, Media, and Communication, 2015, Volume 3, Issue 2.
2. Gaydareva I.N, Eshev M.A. Markov P.N., Internet Censorship in the Context of Legal Regulation in Russia, Advances in Economics, Business and Management Research, 2020, volume 138.
3. William Bendix and Paul J. Quirk, Secrecy and negligence: How Congress lost control of domestic surveillance, Issues in Governance Studies, March 2015.

C. Laws& regulations

1. The (dissolved) Coalition Provisional Authority Order No. 65 of 2004, the High Commission for Communications and Information, March 20, 2004. .(In Arabic).
2. (Dissolved) Coalition Provisional Authority Order No. 68 of 2004, Ministerial Committee on National Security, April 4, 2004. .(In Arabic).
3. Law No. (16) of 2019 Cyber Security Law, Jordan, Official Gazette 2019. .(In Arabic).
4. Law No. 175 of 2018 on Combating Information Technology Crimes. Published in the Official Gazette, Issue (32) on August 14, 2018. .(In Arabic).
5. Egyptian Cabinet Resolution No. 2259 of 2014 establishing the Supreme Council for Cyber Security. .(In Arabic).
6. Court of Justice of the European Union, Press Release, No 54/14, Luxembourg, 8 April 2014.
7. Royal Order No. 6801 on February 11, 1439 AH, regulating the National Cyber Security Authority in the Kingdom of Saudi Arabia. .(In Arabic).
8. Russian Federation, Personal Data, law No 152 FZ, 14 July 2006.
9. Socialist Republic of Vietnam, Law on Cybersecurity, No.: 24/2018/QH14, 12 June 2018.