HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير العربي للعام 2024 = 0.44

عنوان البحث

الواقع التشريعي للأمن السيبراني في العراق: التحديات والطموحات

محمد كاظم هادي عنجور المنصوري[1]

[1] باحث، العراق.

بريد الكتروني: qasim.93.r@gmail.com

HNSJ, 2025, 6(8); https://doi.org/10.53796/hnsj68/36

المعرف العلمي العربي للأبحاث: https://arsri.org/10000/68/36

تاريخ الاستقبال: 2025/07/07م تاريخ القبول: 2025/07/15م تاريخ النشر: 2025/08/01م

المستخلص

يتناول هذا البحث مفهوم الأمن السيبراني في العراق، مسلطًا الضوء على التحديات التي تواجهها البلاد في ظل التحولات الرقمية السريعة. يعاني العراق من ضعف في البنية التحتية الرقمية ونقص في التشريعات القانونية اللازمة لحماية الأمن السيبراني، مما يجعله عرضة للاختراقات والهجمات الإلكترونية. كما يشير البحث إلى تصاعد التهديدات السيبرانية، مما يتطلب استجابة قانونية وتقنية فعالة. توصي الدراسة بضرورة تطوير إطار قانوني شامل، وتعزيز البنية التحتية الرقمية، وزيادة الوعي بأهمية الأمن السيبراني بين صانعي القرار والمجتمع. كما تدعو إلى إنشاء مركز وطني متخصص للأمن السيبراني لتعزيز جهود الحماية والتنسيق على المستوى الوطني.

الكلمات المفتاحية: الأمن السيبراني، التحديات الرقمية، البنية التحتية الرقمية، التشريعات القانونية، الهجمات الإلكترونية.

RESEARCH TITLE

The Legislative Reality of Cybersecurity in Iraq: Challenges and Ambitions

Abstract

This research addresses the concept of cybersecurity in Iraq, highlighting the challenges faced by the country amid rapid digital transformations. Iraq suffers from weak digital infrastructure and a lack of adequate legal frameworks to protect cybersecurity, making it vulnerable to breaches and cyberattacks. The study also points to the escalating cyber threats, necessitating effective legal and technical responses. The research recommends developing a comprehensive legal framework, enhancing digital infrastructure, and raising awareness of cybersecurity importance among decision-makers and society. Additionally, it calls for the establishment of a specialized national cybersecurity center to strengthen protection efforts and coordination at the national level.

Key Words: Cybersecurity, Digital Challenges, Digital Infrastructure, Legal Legislation, Cyber Attacks.

مقدمة

في ظل التحوّلات المتسارعة التي يشهدها العالم في مجالات التكنولوجيا والاتصالات، أصبح الفضاء الرقمي جزءاً لا يتجزأ من حياة الأفراد والدول، ما أفرز تحديات أمنية غير مسبوقة تمثلت في الجرائم الإلكترونية والتهديدات السيبرانية. هذه التحديات أوجدت ضرورة مُلحّة لصياغة مفاهيم وأطر قانونية جديدة قادرة على مواكبة هذا الواقع المتغير، كان في مقدمتها مفهوم "**الأمن السيبراني**"، الذي لم يعد خيارًا بل ضرورة لحماية الأمن الوطني ومؤسسات الدولة الحيوية. يكتسب هذا الموضوع أهمية خاصة في الحالة العراقية، حيث أدّت هشاشة البنية التحتية الرقمية بعد عام 2003، وغياب التشريعات المواكبة، إلى جعل البلاد عرضة للاختراقات والهجمات الإلكترونية. وعليه، يسعى هذا البحث إلى استقصاء مفهوم الأمن السيبراني من جوانبه اللغوية والقانونية والتقنية، وتحليل واقعه في العراق، في ضوء التحديات القائمة والجهود التشريعية المبذولة، وذلك من خلال دراسة تحليلية نقدية تهدف إلى الوقوف على مكامن الضعف واقتراح المعالجات القانونية اللازمة لتعزيز الحماية السيبرانية.

أهمية البحث

تكمن أهمية هذا البحث في تسليط الضوء على مفهوم الأمن السيبراني وضرورة تنظيمه قانونيًا لمواجهة التحديات الرقمية المتزايدة. كما يبرز أهمية وضع تشريعات وطنية تحمي البنى التحتية الحيوية في العراق من الهجمات الإلكترونية. يساهم البحث في توعية صانعي القرار بخطورة الفجوة القانونية في هذا المجال. كذلك يُعد مرجعًا أكاديميًا يعزز الدراسات المستقبلية المتعلقة بالأمن الرقمي والسيبراني.

إشكالية البحث:

مع التوسع المتسارع في استخدام التكنولوجيا الرقمية في العراق، برزت الحاجة الملحة إلى وجود إطار قانوني متين ينظم الأمن السيبراني ويحمي الأفراد والمؤسسات من التهديدات الإلكترونية المتزايدة. إلا أن الواقع التشريعي الحالي يعاني من قصور واضح، مما يطرح تساؤلات حول كفاية القوانين الحالية لمواجهة هذه التحديات.

أسئلة البحث:

1. إلى أي مدى يُعد الإطار القانوني العراقي الحالي كافيًا لمواجهة التحديات المرتبطة بالأمن السيبراني؟
2. ما أبرز أوجه القصور في التشريعات العراقية المتعلقة بالأمن السيبراني مقارنةً بالمعايير الدولية؟
3. ما هي أهم المخاطر والتحديات السيبرانية التي تواجهها المؤسسات العراقية في ظل غياب تشريع شامل؟
4. كيف يمكن تطوير المنظومة القانونية العراقية لضمان حماية فعّالة للبنية الرقمية وحقوق الأفراد في الفضاء السيبراني؟

منهجية البحث

يعتمد هذا البحث على المنهج الوصفي التحليلي، حيث يسعى إلى دراسة وتحليل الإطار القانوني الحالي للأمن السيبراني في العراق من خلال جمع البيانات والمعلومات المتعلقة بالتشريعات الوطنية والدولية ذات الصلة. كما سيتم تحليل القوانين العراقية المقارنة مع المعايير الدولية لتحديد نقاط القوة والقصور.

هيكلية البحث:

المبحث الأول: مفهوم الامن السيبراني

المبحث الثاني: الامن السيبراني في القانون العراقي

المبحث الأول

مفهوم الامن السيبراني

في ظل التطور الهائل في تكنولوجيا المعلومات والاتصالات، برزت تحديات أمنية جديدة تستهدف الفضاء الرقمي، مما أفرز نمطاً مستحدثاً من الجرائم أُطلق عليه "الجرائم الإلكترونية". وقد اقتضى هذا الواقع المتغير استحداث مفاهيم وآليات حماية جديدة، كان من أبرزها مفهوم "الأمن السيبراني"، الذي بات يشكل الإطار الناظم لمواجهة هذه التهديدات وضمان سلامة الفضاء الرقمي. وفي هذا السياق، يتطلب فهم الأمن السيبراني الوقوف على معناه اللغوي والاصطلاحي، من خلال تحليل مفردتي "الأمن" و"السيبرانية" كلٌّ على حدة، وذلك لبيان الخلفية المفاهيمية التي يرتكز عليها هذا المجال الحيوي في الواقع القانوني المعاصر.

المطلب الأول: تعريف الامن السيبراني

الأمن لغة واصطلاحاً

اولاً: تعريف الأمن لغةً:

إنه عكس الخوف. الفعل الثلاثي آمن، أي تحقيق الأمان، اعتقدت، لأني آمن، وحميت الآخرين، وهو ضد خوفي، فالأمن ضد الخوف، والثقة ضد الخيانة، والإيمان ضد الكفر، والإيمان يعني. التأكيد، وضدها الإنكار، فيقال يؤمن به الناس ويكذبون فيه.[1]

فلان أمنةٌ أي يأمن كل أحد ويثق به، ويأمنه الناس ولا يخافون غائلته.

وقوله تعالى: ﴿ وَعَدَ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ وَعَمِلُوا الصَّالِحَاتِ ﴾.[2]

وقوله تعالى: ﴿و إِذْ جَعَلْنَا الْبَيْتَ مَثَابَةً لِلنَّاسِ وَأَمْنًا ﴾.[3]

الأمن هو أحد مؤشرات الإيجابية الإنسانية، والتعالي، والتفوق، والقدرة على خلق الظروف المثالية لعيش سلمي. بالمقابل، فإن انهيار الأمن وتدهوره يدل على سلبية الإنسان وأنانيته، فضلاً عن سعيه الدؤوب إلى التملك، على المستويين الفردي والجماعي، مما يؤدي إلى الاعتقاد بأن الأمن هو سر الحياة والتنمية. التطور والتطور.

وجاء بمعنى التصديق: فأصل الإيمان التصديق وهو مصدر آمن يؤمن إيماناً، فهو مؤمن.

كما عرّف الأمن على أنه: الأمن رفيق ضد الخوف، والأمان بالفرح، والأمن كفرصة، والأمان كحركة، كل هذه الأشياء آمنة ومأمونة، تمامًا مثل الفرح والأمير، ورجل آمن مثل الرجل. حمزة، ينقلون أمن الجميع في كل شيء.[4]

الأمن هو الشعور بالأمن والاستقرار الذي يمكّنه الفرد والجماعات التي يتألف منها المجتمع من تحقيق وإنتاج المزيد.،[5] وبمعنى آخر جاء كلمة الأمن بمعنى الحفظ أن الأمنة وهي جمع أمين هم الحفظة، وأصل الحفظ الأمن من خوف الضياع.[6]

---

[1] ابن منظور، لسان العرب: ص 140

[2] سورة النور: 55

[3] سورة البقرة: 125

[4] الفيروز آبادي، القاموس المحيط: ج 4: ص 197

[5] عبد الحميد، الاستراتيجية الأمنية والتحديات المعاصرة: ص 25

[6] عمر، معجم اللغة العربية المعاصرة: ج 1: ص 122

ثانياً: تعريف الأمن بصورة مجردة: قدرة الدولة على تحديد إمكانياتها وقوتها الداخلية والخارجية، ومعايير هذه القوة اقتصادياً وسياسياً وعسكرياً، كل ذلك للدفاع عن استقرار الدولة. على المستويين الدولي والمحلي.

هو التأكيد على أن الشخص يمتلك إيمانه، ونفسه، وعقله، وعائلته، وجميع حقوقه، وأنه ليس خائفًا في هذا الوقت أو في المستقبل، داخل أو خارج بلده، أو العدو أو آحرون. وذلك وفق هدى الإسلام وهدى الوحي والتمسك بالأخلاق والعادات والواجبات..[7]

توصف بأنها: الإجراءات التي تتخذها الدولة في حدود قدرتها على الحفاظ على هويتها ومصالحها في الحاضر والمستقبل، مع مراعاة التطورات الدولية..[8]

كان يعتقد أن الأمن هو قدرة الدول والمجتمعات على الحفاظ على تكوينها المستقبلي ووحدتها الوظيفية ضد قوى التغيير التي اعتبروها معادية في سعيهم لتحقيق الأمن. أساس الأمن هو البقاء، لكنه يشمل أيضًا عددًا من الاهتمامات الأساسية حول ظروف الوجود. لا يعني السعي وراء التحرر من التهديدات. في اللاسلطوية، الأمن مشروط ولا يمكن الاعتماد عليه.

وعرف بأنّه عدم توقع المكروه في الزمان الآتي[9]

هذا كل شيء: التأهب والأمن من خلال حماية الضروريات الخمس من أي هجوم. ونتيجة لذلك، فإن أي شيء يشير إلى معنى الراحة والرضا، وكذلك توفير السعادة والتقدم في أي جانب من جوانب الحياة هو الأمان..

بأنّ أصل الأمن، هو: سكون القلب عن توقع الضرر، فهو آمن، وأمن، وأمين.

بأنه مجموعة الاجراءات والسياسات التي تتخذها دولة ما لحماية شعبها وكيانها وانجازاتها.

ووصفها روبرت ماكمار: إنها تشير إلى التنمية والتنمية الاقتصادية والاجتماعية والسياسية على أساس عدم نشاط المحتوى. يقول: إن الأمن الفعلي لدولة ما ينبع من معرفتها العميقة بالمخاطر التي تهدد قدراتها المختلفة والتصدي لتلك المخاطر لتعزيز تلك القدرات في جميع المجالات.

أمن فقهاء المسلمين هو ما يطمئن الناس على عقيدتهم وأنفسهم وأموالهم وشرفهم، ويتركز تفكيرهم على زيادة قيمة مجتمعهم والنهوض بوطنهم.

إنها حالة التوازن التي يجب أن تشمل المنطقة ككل، دون أي تهديد، داخلي أو خارجي.

وصفها ريموند آرون بهذه الطريقة: في حالة الطبيعة، يكون الأمن هو الأولوية الأولى لكل فرد أو كيان سياسي، ويعتمد المستوى الفعلي للأمن على هذا: الأهداف الأبدية، والإدراك الواقعي للأمن يقتصر على البقاء. للدولة، في المقام الأول..

إنه الشعور الفردي والإنساني الجماعي بإشباع حاجاتهم العضوية والنفسية، وعلى رأس القائمة احتياجات الأمن مع ظهور مادي ونفسي، والمتمثل في تأكيد المجتمع على عدم وجود خطر على المجتمع. إن مظهر هذا الدافع المادي، مثل السكن والدخل الحالي، له أيضًا عنصر نفسي، يتم التعبير عن دور الفرد ومكانته في المجتمع في البيان العام للهدوء طوال فترة حياة المجتمع بهدوء.

---

[7] الخادمي، «القواعد الفقهية المتعلقة بالأمن الشامل»: ص 16

[8] أمين، الأمن العربي في مواجهة الأمن الاسرائيلي: ص 42

[9] المناوي، التوقيف على مهمات التعاريف: ج 1: ص 55

السيبرانية لغة واصطلاحاً

أولاً: السيبرانية لغة: كان مرتبطًا بمعنى كلمة cyber، وكان يُعتقد أنه نشأ من اليونانية ويشار إلى مصطلح (kybernetes)، والذي يعني القيادة أو التحكم عن بعد..[10] وجاء في قاموس المرد بانها علم الضبط ومصدرها اي ضبط الاشياء عن بعد والسيطرة عليها.

ثانياً: السيبرانية اصطلاحاً: مشتق من كلمة *cyber*، وهي صفة تصف أي شيء مرتبط بثقافة الكمبيوتر أو التكنولوجيا أو الواقع الافتراضي. السيبرانية تعني المساحة الافتراضية للإنترنت.

أصبح الأمن السيبراني محور التقنيات الإضافية التي توسعت فيه..[11]

وصل الأمن السيبراني إلى مرحلة حرجة حيث التقنيات التي وسعت الآفاق، وأثريت الثقافة، وسمحت للثقافة المحلية بالانتشار إلى المجال العالمي، تشكل الآن تهديدًا للهوية الوطنية والثقافية، والأفراد الأكثر ضعفًا هم أولئك الذين يتأثرون بها. ما يصلون إليه عبر الإنترنت، عبر التكنولوجيا، ورغبة الغالبية العظمى في استخدامه لتشكيل مجتمعهم الخاص.

تم اعتبار سلامة الشبكة والبيانات والمعلومات والأجهزة المتصلة بالإنترنت، وكذلك المعايير الواجب اتباعها لمواجهة التهديدات ومنع التعديات والحد من خطورة آثارها في معظم الحالات. المواقف المتطرفة والضارة..[12]

وصفت التوصية الأوروبية، التي صدرت عام 2002، الأمن القومي بأنه أمن الدولة، والدفاع، والسلامة العامة .... ونتيجة لذلك، فإن الأمن القومي هو الحماية الكاملة لأي بلد من أي نوع من التهديد أو الخطر الذي قد يعرض سلامة مواطنيها أو أراضيها أو سيادتها للخطر. وهذا يشمل حماية البنية التحتية الحيوية أو الاتصالات أو المعلومات.

يصف ريتشارد كيمير الأمن السيبراني بأنه استباقي لمشكلة تكتشف وتكافح محاولات المتسللين للتسلل.

تصف وزارة الدفاع الأمريكية الفضاء الإلكتروني بأنه: فضاء افتراضي يتميز باستخدام الإلكترونيات (أي تكنولوجيا المعلومات) والطيف الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات عبر شبكات الاتصالات والبنية التحتية المادية المرتبطة بها.[13]

كما توصف بأنها مجموعة من الإجراءات الفنية والإدارية المستخدمة لمنع الوصول غير المصرح به واستعادة المعلومات الإلكترونية المفقودة وأنظمة الاتصال والمعلومات من أجل ضمان وظائف وخصوصية البيانات الشخصية. بالإضافة إلى ذلك، من الضروري اتخاذ جميع الخطوات اللازمة لحماية المواطنين.

وصفها إدوارد أمورسو بأنها: تُعرَّف على أنها: تساعد على منع الهجمات على البرامج أو الأجهزة أو الشبكات. تتضمن هذه الأساليب أدوات تهدف إلى مكافحة القرصنة واكتشاف الفيروسات ومنعها..

إنها مجموعة من الإجراءات التنظيمية والإدارية التي يتم استخدامها لمنع الوصول غير المصرح به، والهدف من ذلك هو ضمان استمرار توافر النظام وسريته، وحماية البيانات الشخصية، واتخاذ الإجراءات لحماية المواطنين والمستهلكين من الخطر..[14]

التقرير السنوي للاتحاد الدولي للاتصالات عن إصلاح الاتصالات لعام 2010–2011 هو عبارة عن تجميع للمهام

---

[10] الفتلاوي، «الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر»: ص 614

[11] الربيعة، «الأمن الرقمي وحماية المستخدم من مخاطر الانترنت».

[12] جبور، السيبرانية هاجس العصر: ص 260

[13] لين، «النزاع السيبراني في القانون الدولي الإنساني»: ص 516

[14] عبد الرضا والمعموري، «الامن السيبراني ودورة في انتشار ظاهرة الارهاب في العراق بعد العام 2003م»: ص 154

بما في ذلك إنشاء أدوات وسياسات وإجراءات أمنية ومبادئ توجيهية وطرق للتعامل مع التهديدات السيبرانية، والتدريب، والممارسات والأساليب النموذجية. يمكن توظيفها لحماية الفضاء السيبراني وموارد المنظمات والمستخدمين..[15]

وقد تم تعريف الامن السيبراني: بأنه النشاط او العملية او العملية القدرة او الامكانية التي يتم بموجبها حماية نظم المعلومات والاتصالات والمعلومات الواردة فيها او الدفاع عنها ضد الضرر او الاستخدام غير المصرح به او الاستغلال.

الفضاء السيبراني

الفضاء الإلكتروني هو مجال افتراضي يستخدم أنظمة الكمبيوتر واتصالات الإنترنت وكمية كبيرة من البيانات والمعلومات والأجهزة. كما يعرّف آخرون الفضاء الإلكتروني بأنه ذراع للجيوش الحديثة يحتل المرتبة الرابعة من حيث الأهمية.

تصفه الوكالة الفرنسية للأنظمة الأمنية على أنه: مساحة معالجة البيانات الرقمية التي تم إنشاؤها بواسطة الاتصال العالمي للمعدات للمعالجة التلقائية..

يصف تعريف الاتحاد الدولي للاتصالات للفضاء السيبراني أنه الفضاء المادي وغير المادي الذي يتكون من العناصر: أجهزة الكمبيوتر والشبكات والبرمجيات ومعالجة المعلومات والمحتوى وبيانات الإرسال والتحكم، ومستخدمي كل هذه المكونات..

جوزيف ملزم بكلمته. ناي هو أحد أبرز الأفراد المهتمين بالقوة السيبرانية، وهو يعرفها على النحو التالي: القدرة على تحقيق النتائج المرجوة من خلال استخدام موارد المعلومات المرتبطة بالفضاء السيبراني، وهذا يعني أن القوة السيبرانية هي القدرة على الاستفادة الفضاء الإلكتروني لجني فوائد للدولة، وللتأثير على الأحداث في بيئات تشغيلية أخرى من خلال الأدوات القائمة على الإنترنت ..

المطلب الثاني: اهداف وخصائص الامن السيبراني

أهداف الامن السيبراني: تهدف الى الحفاظ على قدرات الامن الوطني التكنولوجي وتامين البيانات الحيوية بما يساهم في تحقيق الامن السيبراني وتحديد اهداف الدفاع الالكتروني كالتالي:[16]

حماية القواعد العسكرية.

أمن البيانات العسكرية.

حماية البنية التحتية الأكثر حيوية.

مساعدة وحدات الحرب الإلكترونية.

العقوبة الإلكترونية.

نتيجة لذلك، يجب على المؤسسات والأفراد محاولة ضمان أمن الاتصالات، من خلال الحفاظ على سريتها، وهناك قضايا مرتبطة بذلك، بما في ذلك مكافحة الجريمة والحفاظ على الأمن. هذا هو السبب في أن الأمان يمنع المستخدمين من استخدام النظام باستثناء ما هو مقصود، وضمن المعلمات المسموح بها..[17]

---

[15] جبور، «الامن السيبراني التحديات ومستلزمات المواجهة»: ص 3

[16] كلاع، «الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني»: ص 306

[17] فورة، جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية: ص 4

ابعاد الامن السيبراني: ان امن السيبراني متكاملة تعمل على حفاظ على الامن القومي من كل التهديدات السيبرانية كالاتي.[18]

المكون العسكري.

البعد الاجتماعي.

البعد الاقتصادي.

البعد القانوني.

المكون السياسي.

خصائص الأمن السيبراني: الحرب الإلكترونية هي نتيجة مباشرة للثورة الرقمية والإلكترونية في الشؤون العسكرية. إنه شن هجمات على أنظمة تكنولوجيا المعلومات الحاسمة للخصم وتدميرها بأسلحة تقليدية أو غير تقليدية في العصر الحديث..[19]

وعند توفر بشكل متزايد في شتى مناحي الحياة والمصالح الحيوية حول العالم التحول نحو الرقمنة اعتمده على الفضاء الالكتروني والصحة والتعليم والمؤسسات والمعاملات الحكومية.

بسبب الخصائص والفوائد المحددة لهذه الصراعات، كانت مختلفة عن الحروب التقليدية. ونتيجة لذلك، تختلف قواعد الاشتباك في هذه النزاعات عن قواعد الاشتباك في الحروب التقليدية، حيث يسود التجسس والاستطلاع وجمع المعلومات وتطوير البرمجيات وتجنيد القراصنة.

تتسم الهجمات السيبرانية بخائص تميزها عن غيرها من الهجمات العادية ومن ابرزها ما يلي:

الهجمات السيبرانية هي هجمات تقنية متطورة سهلتها ثورة المعلومات.

يمكن أن يحدث الهجوم السيبراني في أي وقت، ولمدة وجيزة، سواء أثناء الحرب أو السلم.

يتمتع المهاجم بميزة كبيرة في الهجمات الإلكترونية على المدافع، وتتميز هذه الهجمات بالسرعة والتنوع والمراوغة.

التكلفة المنخفضة نسبيًا للهجمات الإلكترونية، والتي تخصص ميزانيات كبيرة لإنتاج أسلحة إلكترونية متطورة بتكلفة عالية، مثل حاملات الطائرات المتقدمة.

كما تتميز الهجمات السيبرانية بالتدمير الذي لا يصاحبه بالضرورة دم أو أجزاء من الجسم، وذلك بسبب انتشار الفضاء السيبراني وسهولة الوصول إليه. الهجمات السيبرانية هي هجمات تقنية متطورة سهلتها ثورة المعلومات.

يمكن أن يحدث الهجوم السيبراني في أي وقت، ولمدة وجيزة، سواء أثناء الحرب أو السلم.

يتمتع المهاجم بميزة كبيرة في الهجمات الإلكترونية على المدافع، وتتميز هذه الهجمات بالسرعة والتنوع والمراوغة.

التكلفة المنخفضة نسبيًا للهجمات الإلكترونية، والتي تخصص ميزانيات كبيرة لإنتاج أسلحة إلكترونية متطورة بتكلفة عالية، مثل حاملات الطائرات المتقدمة.

[18] عبد الصادق، «القوة الإلكترونية: اسلحة الانتشار الشامل في عصر الفضاء الإلكتروني»: ص 32

[19] كلارك، وكنيك، حرب الفضاء الإلكتروني: الخطر القادم على الأمن القومي وسبل مواجهته: ص 286

كما تتميز الهجمات السيبرانية بالتدمير الذي لا يصاحبه بالضرورة دم أو أجزاء من الجسم، وذلك بسبب انتشار الفضاء السيبراني وسهولة الوصول إليه..[20]

– صعوبة تحديد هوية مرتكب الهجمات الإلكترونية عالية التأثير.

تفتقر الهجمات الإلكترونية إلى القيود الجغرافية، حيث تتنوع أساليبها وترتبط بالمجالات المتقدمة والمتغيرة في الحياة المعاصرة في العديد من البلدان.

حسب دراسة ديفيد سميث، بعنوان كيف تستخدم روسيا الحرب الإلكترونية؟ أنظمة الاتصالات والملاحة، والضغط النفسي، وكذلك الدعاية وإلحاق الضرر بنظم المعلومات.

مستخدمو وسائل التواصل الاجتماعي (Facebook كمثال) لديهم مؤخرًا أكثر من 1.5 مليار مستخدم نشط، وتشير الإحصائيات الأخيرة إلى أن عدد العرب الذين يستخدمون الموقع قد ارتفع إلى ما يقرب من 100 مليون، ويستخدم جزء كبير من هذا العدد الهواتف الذكية الحديثة..[21]

تشفير التعاملات الإلكترونية بحيث لا يستطيع أي مخترق أو مهاجم أو عابث أن يدخل بسهوله لهذه البيانات والتطبيقات لان التشفير أحد أساليب الحماية والتي يصعب فك رموزها.

تعنبر التشفير وسيلة لحفظ سرية المعلومات وتحويل الرسائل الى نصوص مشفرة لكي يصعب على اي شخص قراتها فلا يمكن معرفة فحوى المعلومات المرسلة من قبل اي شخص آخر غير الشخص المرسل له تلك المعلومات في حالة وصول تلك المعلومات الى اشخاص آخرين فانهم لا يستطيعون الاستفادة منها او حتى فهم معناها.

إقرار التشريعات الملائمة لتشجيع الانخراط السليم والأمن، في مجتمع المعلومات، والاستفادة من آفاق مجتمع المعرفة، بما يخدم النمو والتنمية، لا سيما فيما يتعلق بها.

منصة التجارة الإلكترونية

حماية الخصوصية والحق في الكلام.

ضمان الوصول إلى شبكة واسعة من المعلومات.

– سلامة المعلومات الشخصية، وخاصة المعلومات الحساسة.

تنظيم المحتوى.

– حماية حقوق الملكية الفكرية.

ضمان سلامة الأطفال على الإنترنت.

تنظيم المعاملات الإلكترونية.

توزيع المهام والاستفادة من الخدمات السحابية.

– اعتماد قواعد التجريم الموضوعية.

---

[20] العبودي، «هاجس الحروب السهيبرانية وتدا ياتها على الأمن والسلم الدوليين»: صص 89–118

[21] هشام، «جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة»: ص 61

– إرساء مبادئ الملاحقة والتحقيق وتنفيذ الجرائم الإلكترونية.

– تنفيذ الاتفاقيات الوطنية والإقليمية والدولية.

– تنفيذ التشريعات المناسبة التي تسهل التعاون بين القطاعين العام والخاص في مكافحة الجريمة السيبرانية.

فيما يتعلق بالجرائم العابرة للحدود، تعتمد الدول الأعضاء على مبدأ توحيد القواعد القانونية لتجريم الأفعال المرتبطة بالجرائم الإلكترونية، ومبادئ الملاحقة والتنفيذ، حتى تتبنى كل دولة القواعد القانونية التي تسمح لها بتبني هذا المبدأ. من الجرم المضاعف، وذلك لتسهيل التعاون وتفعيله.

المبحث الثاني

الامن السيبراني في القانون العراقي

مع التطور المتسارع في مجال تكنولوجيا المعلومات والاتصالات، أضحى الأمن السيبراني عنصرًا أساسيًا في حماية البنى التحتية الرقمية للدول، لا سيما مع تزايد التهديدات والهجمات الإلكترونية العابرة للحدود. وقد بات العراق، بعد عام 2003، يواجه تحديات أمنية رقمية متنامية نتيجة ضعف البنية التحتية التقنية، وانكشاف منظوماته الحكومية والمؤسساتية أمام موجات من القرصنة والتجسس السيبراني. وعلى الرغم من أهمية الأمن السيبراني كرافعة لحماية الأمن الوطني، إلا أن التشريعات العراقية لا تزال تعاني من نقص في التكيّف مع الواقع السيبراني، سواء من حيث التنظيم القانوني أو من حيث الأدوات والمؤسسات المعنية بالمواجهة. في هذا المبحث، سيتم تناول واقع الأمن السيبراني في العراق من خلال استعراض التدهور الحاصل في هذا المجال، وتحليل مدى استجابة القانون العراقي للمتغيرات التكنولوجية، وتسليط الضوء على الجهود التشريعية المبذولة لمكافحة الجرائم الإلكترونية ومظاهر الإرهاب السيبراني.

المطلب الأول: التدهور السيبراني في العراق

يعاني العراق كل يوم من تبعات الفساد والفوضى وغياب التخطيط الفعال من قبل المسؤولين عن مؤسسات الدولة في العراق. على الرغم من الميزانيات الكبيرة والقدرات المالية المخصصة للمشاريع، والتي لا يزال الكثير منها خططًا افتراضية عالقة على الورق دون أن يكون لها أي شيء، لا تزال الدولة تفتقر إلى تطوير عقيدة تتماشى مع جميع التحديات المستقبلية المرتبطة بالفضاء السيبراني. الأمن، على عكس أمن المعلومات، وهما مصطلحان منفصلان. لا ينبغي الخلط بينهما ... على الرغم من التأثير الإيجابي والهام الذي لوحظ على الحياة الفردية والاجتماعية نتيجة للثورة التكنولوجية والمعلوماتية، وكذلك تطور التواصل الاجتماعي، فقد أدى ذلك إلى تطوير عمليات البحث العلمي وتقليص الوقت اللازم للوصول والحصول على المعلومات. نتيجة لذلك، نناقش الآن التجارة الإلكترونية والصحة الإلكترونية وكذلك الحكومة الإلكترونية والصحافة الإلكترونية. لكن هذا لا يعفيها من تأثيرها السلبي على الأمن الوطني والدولي، فقد أصبحت تحديًا وتهديدًا خطيرًا، مما يعني أن دائرة التهديدات للأمن الوطني والإقليمي تشهد الآن نوعًا جديدًا من الصراع الدولي..[22]

عندما يُلاحظ أن للفضاء الإلكتروني تأثير كبير على معظم مجالات حياتنا، بما في ذلك المجال الأمني ، فإن الفضاء الإلكتروني يستخدم أدواته المختلفة لإعادة رسم البعد الأمني المحلي والعالمي، وهذا يؤدي إلى تغيير في الوعي السياسي والأمني للفرد والمجتمع.، الطريقة التي تقوم بها بهذا الأمر تختلف عما كانت عليه في السابق. نلاحظ تصورات وهياكل جديدة يتم إنشاؤها في المجالات السياسية والأمنية، حيث لم يعد الأمن موجودًا في العالم الحقيقي – المحدود –

[22] العوادي، «حماية الأمن السيبراني العراقي الاستراتيجية المفقودة»

ولكن بدلاً من ذلك في الواقعية واللامحدودة التي أصبح الفضاء الإلكتروني لها وجودًا مؤثرًا في المجال الأمني ، المناقشة مراكز حول الحرب الإلكترونية، والأمن السيبراني، والردع السيبراني، والجيش السيبراني، والأسلحة الإلكترونية، والإرهاب السيبراني، والجريمة الإلكترونية. كانت هذه المؤسسات مهتمة في المقام الأول بدراسة الفضاء الإلكتروني وكيفية الاستفادة منه بطريقة تعزز أهدافها السياسية والأمنية والاقتصادية. إلخ، بحيث يتمثل التهديد المستقبلي للفضاء السيبراني في قدرة الدول على التكيف مع التغيرات والتحديات السريعة في الفضاء السيبراني في المجال العام ككل وفي المجال الأمني على وجه التحديد، فضلاً عن امتلاكها للقدرات والموارد و الهياكل البشرية والمادية التي تسمح لهم بالتأثير والتأثير في الفضاء السيبراني. لا يقتصر تأثير الفضاء الإلكتروني على الأمن على الحقائق الداخلية للدول، بل يؤثر بدلاً من ذلك على البيئة الدولية بطريقة واسعة لتغيير هيكل ومحتوى الأمن الدولي وإنشاء نماذج جديدة لطبيعة العلاقات الدولية وأمن الدولة..[23]

ولم يعرف العراق هذا الفضاء إلا بعد عام (2003)، وشهد زيادة ملحوظة وملحوظة في استخدام المعلومات والاتصالات، تزامن ذلك مع ضعف في الأمن الرقمي للبنية التحتية للبلاد (سواء الوطنية أو المصرفية أو الأمن الشخصي)، مما جعله عرضة للتهديدات الأمنية (سرقة المعلومات). كما أن للولايات المتحدة تاريخ طويل في التجسس على أجهزتها الأمنية والاستفادة منها) من قبل الدول الدولية والإقليمية الكبرى، وكان ذلك أكثر وضوحًا في أعقاب الشكوك التي أحاطت بالانتخابات البرلمانية الأخيرة في مايو 2018، والتي نجمت عن حقيقة أن كان نظام التصويت على القمر الصناعي لا يمكن السيطرة عليه لأنه كان يدار من خارج العراق، مما جعل من السهل اختراقه والتلاعب به. بالمعلومات التي تم الحصول عليها من خلال هذه العملية من قبل أطراف ثالثة لديها التكنولوجيا اللازمة لذلك..[24]

كما أن الولايات المتحدة التي كانت تعلم قبل دخولها المنطقة أن العراق يفتقر إلى هذه التقنيات، بدأت في تنفيذ خططها. في السابق كانت الولايات المتحدة وخططها في البنتاغون تدفع العراق إلى شن حرب على جمهورية الإسلام الإيرانية، وهذا من شأنه أن يستنزف القوى الروحية التي تتشكل على صمود الإيمان. يعتبر مفهوم الحرب الاستباقية أحد نتائج هجمات 11 سبتمبر في الولايات المتحدة في عام 2001، لكن المفهوم الأساسي يسبق هذا التاريخ.، وجاءت هذه النظرية حتى تبرر تصرفات القصف ليبيا التي قامت بها حكومة ريغن، واصبح هذا التبرير هو دفاعا عن النفس وهذا الدفاع هو انه تتوقع تلك القوات بأنها سوف تتعرض في المستقبل الى ضربة عسكرية، فهل يكون ضرب دولة ويتم قصفها على الظن؟؟، وكان ذلك هو تبريرها بأنها تعتبر دفاعا عن النفس ضد هجوم مستقبلي، وكما قامت اسرائيل بنفس الفكرة وكان الهدف من هجماتها على سوريا ومصر والأردن والغاية من منه هو السيطرة على الضفة الغربية وكذلك القدس الشرقية وكذلك قطاع غزة ومرتفعات جولان السورية، أما هجومها على العراق فكان بهدف تحطيم المفاعل النووي العراقي أوزيراك.

المسألة أن العراق ظل عاجزاً عن التقدم بعد سقوط النظام، وأصبح دولة محتلة من قبل أمريكا، ومكاناً للصراع والدمار. انتقد المركز العراقي للإعلام الرقمي ترتيب البلاد في تقرير مؤشر الأمن السيبراني العالمي، مشيراً إلى أنه لا يتماشى مع الإمكانات الفعلية للبلاد. وقال بيان المركز يوم الاحد ان التقرير الاخير للاتحاد الدولي للاتصالات التابع للامم المتحدة وضع العراق في المرتبة 107 عالميا في مجال الامن السيبراني والمرتبة 13 عربيا. تبع ذلك السودان وفلسطين والأردن

حيث انه يتم تعريف التوجه الاستراتيجي اجرائيا: على انه الإطار العام الذي تعتمد عليه منظمات الأعمال في عملية

[23] خريسان، «العراق وتحدي الفضاء السيبراني: قراءة في مؤشر الامن السيبراني العالمي».

[24] العوادي، «حماية الأمن السيبراني العراقي الاستراتيجية المفقودة»

تحديد الأهداف والتوجهات المستقبلية التي تسعى للوصول اليها، وهو أيضا الإطار الذي يضبط ويوجه عملية اتخاذ القرار وذلك من اجل تحقيق التوافق والتكامل بين اهداف المنظمة وسياستها المعتمدة، ويعتبر ذلك من حيث الممارسات الدولية فإنه التغيير في أشكال الحرب الاستباقية ومسمياتها عبر التاريخ لم يغير من جوهرها أو أهدافها، ومن الملاحظ انه تكون هناك افكار مرتبة وجاهزة وفي انتظار ظهور أي ظرف يتلائم مع تحويله إلى خطَّة مفصلة وذلك يكون تمهيدا في تطبيق الفعل، وجاءت تفجيرات البرجين ومبنى وزارة الدفاع في كل من نيويورك وواشنطن، وما إنبثق عنها من مناخ هستيري لتوفير الفرصة المثالية التي ظلت عصابة المحافظين الجدد في انتظارها.[25]

فقد كانت الجيوش تتحرك لغزو أو احتلال أراضي دولة ما للدفاع عن حق دون وجود حاجه إلى إنذار سابق في سعى الدول إلى القضاء على من ينافسها من خصوم كما فعلت روما في حربها مع قرطاج في الآلف الثاني قبل الميلاد. بشكل عام، تعتبر أحداث 11 سبتمبر 2001 إعلانًا عن حروب استباقية، وإذا اعتبرنا تصريحات دبليو بوش في إحدى خطاباته أن الولايات المتحدة ستلجأ إلى الإجراءات الوقائية من أجل منع ما هو متوقع ومتوقع. يعتقد غالبية المحللين والمراقبين أن المبدأ الذي يتبعه بوش هو الحرب الوقائية وليس الحرب الوقائية. كان إيمان بوش بضرورة الحرب الوقائية مبنيًا على ثقته في التفوق الذي لا جدال فيه للقوة العسكرية الأمريكية عالميًا..[26]

المطلب الثاني: السيبرانية في القانون العراقي

تضمن القانون العراقي ومشرعه الذي ورد في قانون العقوبات العراقي رقم (111) الصادر عام 1969، العديد من العقوبات التي لا تزال سارية المفعول حتى اليوم، وتشمل هذه العقوبات النشر والتهديد والأخلاق العامة وغيرها من المواد والنصوص القانونية، جميعها. التي تضمن اتباع ذلك وعدم تجاهله. ومع ذلك، فإن هذا القانون لا يتماشى مع التطور الحاصل أو عدد المشاكل التي تطرأ على المحاكم كل يوم، دون أن يخرج المشرع لوضع الحدود اللازمة التي تمنع أي شخص من محاولة إيذاء الآخرين وكذلك الدولة، المصالح العامة والخاصة. في الوقت الحالي، لا ينطبق تطبيق القوانين الدولية الحالية على الهجمات الإلكترونية إلا بشكل غير مباشر. القانون الدولي يحظر العدوان العسكري ولكن ماذا عن الهجوم السيبراني الذي أدى إلى تفجير القاعدة؟ وهل يجوز للدولة، وفقًا لحقها الطبيعي في الدفاع عن النفس، استهداف أهداف عسكرية في الدولة أو حتى شن هجوم سيبراني مضاد؟ ومع ذلك، لا يزال الجدل قائمًا بشأن القضايا القانونية المحيطة بالهجمات الإلكترونية. نتيجة لذلك، قد يبدو الانتقام عملاً عدوانيًا غير مقصود أو انتهاكًا للقانون الدولي.

يهدف الأمن إلى حماية قنوات الاتصال الرقمية بكل تعقيداتها، وكذلك حماية الشبكات المحلية والعالمية من الاختراق الذي يتسبب في تدمير البنية التحتية لأنظمة المعلومات، بما في ذلك الأجهزة والمعدات وحتى البرامج المالية المختلفة، مثل المال، والطاقة، والإحصاءات، وما إلى ذلك، يتم تحقيق ذلك من خلال اختراق الأنظمة المالية أو اختراقها وتحويل الأموال. وأخذها، وبشكل عام، تحمي تلك الأنظمة من جميع الجرائم المتعلقة بالمعلومات التي تُرتكب بوحشية شديدة. بالإضافة إلى ذلك، فإن الأم خطرة لأن هناك جيوش من المعدات المعقدة والأرقام المخصصة لاختراق الأمن السيبراني للدول المتقدمة والدول التي تفتقر إلى الطاقة، مثل العراق الذي يسيطر على حوالي 11٪ من احتياطيات النفط في العالم ولديه أكبر كمية. من احتياطيات الكبريت والغاز في العالم. ونتيجة لذلك، أصبح العراق الآن بؤرة صراع كبير بين أقوى دول العالم والدول الأخرى التي حاولت دائمًا عرقلة رغبتها في مستقبل أفضل، من أجل جعله سوقًا مفتوحًا لمنتجاتها، والتي لديهم سوق كامل لبضائعهم ويفتقرون إلى الصناعات الوطنية المتقدمة..[27]

---

[25] تشومسكي، الحادي عشر من أيلول الإرهاب والإرهاب المضاد: ص 292

[26] تشومسكي، الحادي عشر من أيلول الإرهاب والإرهاب المضاد: ص 292

[27] الزبيدي، «تهديدات افتراضية للأمن السيبراني العراقي».

من الحقوق الأساسية لكل شخص في العالم حرية التعبير والرأي، والتي تمثل رأي المجتمع وتطلعاته، والتي يتم من خلالها قياس تطور الدول من عدمه. وقد ورد ذلك في النظام الأساسي للدولة (الدستور) في المادة 38: الآداب: أولاً: الحق في إبداء الرأي بأي شكل من الأشكال. ثانياً: حرية الصحافة والطباعة والاعلان والاعلام والنشر. ثالثاً: حرية الاجتماع والتظاهر مقننة بقانون. كما انتشرت، ومن أهم آثار التطور العلمي تكنولوجيا الاتصالات، بدأت هذه التقنية في التطور والانتشار يوماً بعد يوم، حتى أصبحت الشبكة العنكبوتية العالمية (الإنترنت) الوسيلة التي يتم من خلالها نشر الأفكار والآراء في ثوانٍ. ومع ذلك، وعلى الرغم من المساهمة المباشرة لهذه التكنولوجيا في تعزيز حرية التعبير، إلا أنها لم تكن في مأمن من الاستغلال وانتهاك الخصوصية الفردية، ونتيجة لذلك، فإن كل إجراء له رد فعل مضاد، وتنتهي الحرية عندما تنتهي حقوق الآخرين. تم انتهاكهم بقانون ينظمهم من الفوضى.[28]

وان اتجاهات التي تعتبر الإصلاح في الاتصالات للعام 2010–2011، «بانه مجموعة من المهمات، مثل تجميع وسائل، وسياسات، وإجراءات امنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين).

كما أفادت التقارير أن عدد الهجمات القاتلة على الأمن السيبراني العراقي بعد عام 2003 كان الأعلى من حيث اختراق مواقع حكومية معينة. وكان الاعتداء الأخير الذي نفذه رئيس الجمهورية الأسبق السيد إياد علاوي، خلال مقابلة تلفزيونية في نيسان من عام 2018، أقر فيها أن استخدام الأقمار الصناعية في عملية التصويت خلال الانتخابات المقبلة أمر مشكوك فيه لأنه معروف. هذه الأقمار الصناعية مملوكة لدول أجنبية، ولا سيطرة للعراق عليها. بالإضافة إلى ذلك، فإن احتمال القرصنة أو تغيير النتائج مرتفع. لا مخالفات. الآلية هي الإجراءات التي يتم وضعها لمنع التداخل والقوى الخارجية الضارة من التأثير على النتيجة. بالإضافة إلى ذلك، نحتاج إلى السماح بتدقيق تسجيل الصوت، وهذا سيسمح لنا بمناقشة مجموعة كامبريدج. يبدو أن هذه المجموعة من الأفراد لديها القدرة على التسلل إلى برنامج الكمبيوتر المخصص لنقل البيانات، ونتيجة لذلك يمكن أن يكون لها أكبر تأثير سلبي على الأمن السيبراني، والصورة لها التأثير الأكبر على العملية السياسية وهيكل الحكومة، كلاهما يتأثر به بطريقة تفيد المصالح العالمية بدلاً من الناس..؟[29]

وشهد العراق زيادة ملحوظة في الطلب على الشبكات المخصصة للتواصل الاجتماعي، وذلك على ما يبدو لأنه يحتوي على مشروع حضاري يتم التعبير عنه من خلال الحاجة إلى استكمال الخطوات إلكترونياً، وأولها السياسة الإلكترونية الدولية التي يُراد لها أن تكون يُمارس الأمن السيبراني بشكل سلمي وخالي من العنف، كما أُضيف إلى موسوعة الأمن الدولي في جميع المجالات، بما في ذلك العلاقات الدولية، لما له من أهمية كبيرة للأمن القومي للدول على أرض الواقع.

وقال علي الغانمي عضو لجنة الأمن والدفاع النيابية في تصريح لـ (المدى)، إن مجلس النواب سيقرأ تقرير لجنة الأمن والدفاع النيابية بشأن التغييرات في الجرائم الإعلامية. وأوضح الغانمي أن التعديلات جاءت بعد الاتفاقيات، ووصفها بـ تغيير مسمى القانون المقترح من مكافحة الجرائم الإلكترونية إلى الجرائم ضد الحاسوب والإنترنت، وإنشاء المركز الوطني للرقمنة. الدليل الذي سيكون مسؤولاً عن إصدار التقارير التي سيتم اعتبارها دليلاً في المحكمة عند النظر في القضايا المتعلقة بالجرائم الإلكترونية..[30]

---

[28] مهدي، «جريمة النشر الالكتروني وفق القانون العراقي».

[29] الزبيدي، «تهديدات افتراضية للأمن السيبراني العراقي».

[30] صباح، «قانون جرائم المعلوماتية: 21 مادة سالبة للحرية و63 عقوبة حبس وغرامة».

حيث أنهى مجلس النواب القراءة الأولى لقانون جرائم المعلومات العام الماضي والتي تضمنت عقوبات تصل إلى السجن المؤبد وغرامات باهظة على المخالفين ... أوضح ممثل قانون مجلس النواب أنه تم إجراء التعديلات على قانون جرائم المعلوماتية. مشروع 2011 لمخالفته أحكام قانون العقوبات 111 والاتفاقيات الدولية التي توصي بحرية الرأي. ويرى أن القانون أصبح أكثر نضجًا ومتماشيًا مع النهج الديمقراطي، ولا يتعارض مع حرية التعبير، وسيكون له أثر إيجابي على الحياة الاجتماعية للمواطنين.[31].

أعلنت لجنة الأمن والدفاع في مجلس النواب العراقي عزمها على إعادة طرح مشروع قانون جرائم المعلومات الذي يمنح السلطات سلطة مراقبة ومعاقبة المواطنين على منشوراتهم على مواقع التواصل الاجتماعي، وكذلك المشاركة في التصويت على الفاتورة خلال هذه العملية. وركزوا على ضرورة القانون، مؤكدين أنه سيقلل من عدد الجرائم. وسط مخاوف من احتمال إساءة استخدام القانون لقمع التعبير في البلاد ... القانون المثير للجدل مطروح على البرلمان منذ 2018، وقوبل بالتشكيك والمعارضة من قبل نشطاء مدنيين ومدونين في البلاد، بسبب أحكامه التي كانت تعتبر غامضة ومحدودة في التعبير..[32]

في الخامس من حزيران (يونيو) 2022، أعلنت لجنة الأمن والدفاع في مجلس النواب العراقي عزمها على إعادة تقديم مشروع قانون جرائم المعلوماتية، ويمنح القانون السلطات سلطة مراقبة وملاحقة المواطنين على أفعالهم عبر الإنترنت، ولديهم أيضًا القدرة على التصويت. بشأن القانون خلال الدورة التشريعية. في الوقت الحاضر، أكدوا على أهمية وجود القانون من أجل الحد من الجريمة، وذكروا أنه سيتم إساءة استخدام القانون إذا تم استخدامه لقمع حرية التعبير بدلاً من منعها فعليًا. وشهدت محاولات تمرير القانون زيادة أكبر في ختام العام الماضي، قبل أن يتعهد رئيس مجلس النواب العراقي، محمد الحلبوسي، بأنه لن يمرر القانون، وذلك خلال جلسة ضمت ممثلين من دول غربية.

وبحسب عضو لجنة الأمن والدفاع في مجلس النواب النائب ياسر وتوت، فإن لجنته عازمة على سن قانون جرائم المعلومات خلال المرحلة المقبلة. –صباح. وأكد أن اللجنة ستبدأ في عرض فقراتها واحدة تلو الأخرى لمناقشتها قبل تحويلها إلى لجان أخرى لإبداء آرائها. جميع الدول المتقدمة لديها قوانين تحد من الجرائم الإلكترونية وتحافظ على حقوق الجميع، بما في ذلك الحكومة.

الواقع أن المشرع العراقي لم يتمكن من التمييز بين قانون جرائم المعلومات وقانون أمن المعلومات. تعتبر البيانات التي تتم معالجتها لتصبح مخرجات (معلومات) قانون معلومات، وكذلك البيانات التي يتم تنسيقها لتصبح معلومات. بالإضافة إلى ذلك، تعتبر البيانات المدخلات الأساسية التي يجب معالجتها. يعتبر الكمبيوتر معلومات، ولكن قبل إضافته أو تغييره، تعتبر البيانات معلومات إذا كان لها أي نوع من القيمة العملية، مثل الصورة التي يمكن رؤيتها أو النص الذي يمكن قراءته.

المطلب الثالث: الجهود التشريعية العراقية في مواجهة الجرائم الإلكترونية

خرق المشرع العراقي قانون العقوبات العراقي رقم (111) في عام 1969، بارتكاب جرائم ضد الاتصالات السلكية واللاسلكية، وتعريض سلامة الجمهور للخطر، وبالتالي حُكم عليه بالسجن لمدة لا تزيد عن سبع سنوات أو بالسجن لكل من عطل وسيلة اتصال متخصصة بسبب لصالح الجمهور.

وأيضًا من خلال قانون مقترح بشأن جرائم المعلومات تمت صياغته في عام 2018، حددت المادة (2) الأهداف الأساسية التي ينوي تحقيقها.[33]

---

[31] صباح، «قانون جرائم المعلوماتية: 21 مادة سالبة للحرية و63 عقوبة حبس وغرامة».

[32] الكبيسي، «محاولات جديدة لتشريع قانون جرائم المعلوماتية تثير جدلاً في العراق».

[33] المادة (٢) من مشروع قانون جرائم المعلومات لسنة ٢٠١٨

حماية الاستخدام القانوني للكمبيوتر والإنترنت.

ضمان أمن المعلومات وتوفير أكبر قدر من الحماية لأنظمة المعلومات وأجهزة الكمبيوتر والأجهزة والبرامج من التطفل وسوء الاستخدام والتخريب الإلكتروني.

قبة جريمة المعلومات.

الحفاظ على الحقوق المرتبطة بالاستخدام القانوني المشروع لأجهزة الكمبيوتر وشبكات المعلومات

– المحافظة على المصلحة العامة والأخلاق والأخلاق

حماية النظام النقدي للبلاد.

احتوى الدستور العراقي الذي أقره مجلس الأمة في 28 آب 2005 على نص اعتبر جريمة جنائية في كثير من المواضع، حيث أن الدستور من الدساتير التي تنص صراحة على خطر الإرهاب. المادة (7) تنص على ما يلي: ما يلي:[34]

أي كيان أو نهج يحتضن العنصرية أو الإرهاب أو التكفير أو التطهير الطائفي أو يسهله أو يسهله أو يروج له أو يبرره، وتحديداً البعث الصدامي في العراق ورموزه، تحت أي مسمى.

وتلتزم الدولة بمكافحة الإرهاب بجميع أشكاله، وتعمل على منع أراضيها من أن تصبح منصة أو مسارًا أو قاعدة لنشاطها.

وتنص الفقرة الثالثة من المادة (21) على ما يلي: لا يمنح حق اللجوء السياسي إلى المتهم بارتكاب جرائم دولية أو إرهابية أو أضر بالعراق أو تسبب في ضرره..[35]

اما المادة (٧٣) قد نصت على ان يتولى رئيس الجمهورية صلاحيات اصدار العفو بتوصية من رئيس مجلس الوزراء باستثناء ما يتعلق بالعفو الخاص والمحكومين بارتكاب الجرائم الدولية والارهاب والفساد المالي والاداري.[36]

ان المشرع العراقي لم يشر في مضمونة ونصوصه الى الارهاب الالكتروني واثارة على المجتمع، ويشير قانون جهاز مكافحة الارهاب الى ان اهداف هذا الجهاز والقوات التابعة له تدور حول.[37]

مجابهة واستئصال الإرهاب بجميع أشكاله.

تطوير وتنفيذ استراتيجيات شاملة لمكافحة الإرهاب.

الالتزام بالتعاون مع الجهات المختصة بمكافحة الإرهاب.

إنقاذ وتحرير الرهائن من خلال المفاوضات السلمية أو الاعتداء المباشر على مكان الحدث الإرهابي.

العمل مع الوكالات المتخصصة لتنفيذ خطط مكافحة الإرهاب

تبادل ونقل وتقييم المعلومات المتعلقة بمكافحة الإرهاب في العراق وخارجه.

الواجبات الأخرى يجب أن يؤديها رئيس الجهاز، وبموافقة اللجنة الوزارية للأمن الوطني.

غالبًا ما يتسبب في حدوث هجمات على الشبكات والإنترنت. الجرائم الإلكترونية هي جريمة جديدة ترتبط بشكل أساسي

---

[34] المادة (٧) من الدستور العراقي الدائم لسنة ٢٠٠٥

[35] المادة (٢١) من الدستور العراقي الدائم لسنة ٢٠٠٥

[36] المادة (٧٣) من الدستور العراقي الدائم لسنة ٢٠٠٥

[37] المادة (٣) الفصل الاول من قانون جهاز مكافحة الارهاب لسنة ٢٠٠٨

بأنظمة المعلومات، يرتكبها مجرم بارز يمتلك المعرفة اللازمة لكيفية عمل النظام واستغلاله في أعماله غير القانونية، وعادة ما يتم استبدال هذه الجرائم بالمال أو الحقوق الأخرى، ولكن الخطر الأكبر هو أنها يمكن أن تؤدي إلى انهيار اقتصادي، كما حدث في العديد من البلدان بسبب القرصنة المنظمة على البنية التحتية الإلكترونية أو الفشل الأمني بالمعنى السياسي، حيث يمكن أن تؤدي هذه الآثار إلى انهيار أخلاقي واجتماعي.

الخاتمة

في ختام هذا البحث، يتضح أن الأمن السيبراني يشكل تحديًا حيويًا يستوجب اهتمامًا متزايدًا في العراق، خاصةً في ظل التحولات الرقمية المتسارعة التي يشهدها العالم. أظهرت الدراسة أن العراق يعاني من نقص ملحوظ في البنية التحتية الرقمية، بالإضافة إلى قصور تشريعي واضح يعوق تحقيق الحماية الفعالة في المجال السيبراني. كما تؤكد الدراسة تصاعد التهديدات السيبرانية، مما يستلزم اتخاذ خطوات فورية وشاملة لتعزيز الأمن السيبراني الوطني.

النتائج

1. **ضعف البنية التحتية الرقمية** :تعاني العراق من بنية تحتية غير متطورة وغير قادرة على مواجهة الهجمات الإلكترونية المتزايدة، مما يعرض المؤسسات الحيوية لمخاطر جسيمة.
2. **نقص التشريعات المتخصصة** :تشريعات الأمن السيبراني في العراق لا تتسم بالشمولية والحداثة اللازمة لمواكبة التطورات التقنية السريعة، ما يؤدي إلى وجود ثغرات قانونية يسهل استغلالها.
3. **تصاعد التهديدات السيبرانية** :هناك زيادة ملحوظة في وتيرة وتعقيد الهجمات الإلكترونية، والتي تهدد أمن المؤسسات الحكومية والخاصة على حد سواء.
4. **ضعف الوعي القانوني والتقني** :غياب الوعي الكافي لدى صانعي القرار والمجتمع بأهمية الأمن السيبراني يعوق تنفيذ الاستراتيجيات المناسبة.

التوصيات

1. **إصدار تشريعات متطورة وشاملة** :ضرورة تطوير إطار قانوني حديث يواكب المستجدات التقنية، ويحدد بوضوح الجرائم الإلكترونية والعقوبات المرتبطة بها.
2. **تعزيز البنية التحتية الرقمية** :توجيه استثمارات استراتيجية نحو تحديث وتحصين البنية التحتية التقنية، مع التركيز على رفع كفاءة الحماية في المؤسسات الحكومية والخاصة.
3. **رفع مستوى الوعي والتثقيف السيبراني** :إطلاق حملات توعوية مستمرة تستهدف جميع شرائح المجتمع، بالإضافة إلى تدريب وتأهيل الكوادر الأمنية والقانونية المختصة.
4. **تعزيز التعاون الدولي** :العمل على تأسيس شراكات مع الدول والمنظمات الدولية لتبادل المعلومات والخبرات والتنسيق في مكافحة الجرائم الإلكترونية.
5. **إنشاء مركز وطني متخصص للأمن السيبراني** :تأسيس هيئة مركزية ذات كفاءة عالية تكون مسؤولة عن مراقبة وتنسيق جهود الأمن السيبراني على المستوى الوطني.

بتبني هذه التوصيات، يمكن للعراق بناء منظومة متكاملة تضمن حماية أمنه السيبراني، وتعزيز ثقة الأفراد والمؤسسات في الفضاء الرقمي، مما يساهم في تحقيق التنمية المستدامة والاستقرار الوطني.

قائمة الصادر والمراجع

اولاً: المعاجم

1. ابن منظور، محمد بن مكرم. (د.ت). *لسان العرب*. القاهرة: دار المعارف.

2. عبد الحميد، أحمد مختار. (2008). *معجم اللغة العربية المعاصرة*. الرياض: عالم الكتب.

3. الفيروز آبادي، محمد بن محمد (1987). *القاموس المحيط*. بيروت: مؤسسة الرسالة.

ثانياً: الكتب

1. أمين، هويدي. (1975). *الأمن العربي في مواجهة الأمن الاسرائيلي*. بيروت: دار بيروت.

2. تشومسكي، نعوم. (2003). *الحادي عشر من أيلول الإرهاب والإرهاب المضاد*. دمشق: دار الفكر.

3. جبور، مني الأشقر. «السبيرانية هاجس العصر». المركز العربي للبحوث القانونية والفضائية.

4. عبد الحميد، حسن دروش. (1999). *الاستراتيجية الأمنية والتحديات المعاصرة*. القاهرة: دار كتاب المصري.

5. فورة، نائلة عادل. (2014). *جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية*. القاهرة: دار النهضة العربية.

6. المناوي، زين الدين محمد عبد الرؤوف بن تاج العارفي (1990). *التوقيف على مهمات التعاريف*. تحقيق: عبد الخالق ثروت. القاهرة: عالم الكتب.

ثالثاً: البحوث

1. اسعد، طارش عبدالرضا وعلي ابراهيم مشجل المعموري، (٢٠٢٠). «الامن السيبراني ودورة في انتشار ظاهرة الارهاب في العراق بعد العام 2003م». دراسات دولية (80)

2. جبور، الشقر منى. (2012). «الأمن السيبراني التحديات ومستلزمات المواجهة». بحث مقدم للمركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، اللقاء السنوي الأول للمختصين في أمن وسالمة الفضاء السيبراني.

3. الخادمي، نور الدين. (د.ت). «القواعد الفقهية المتعلقة بالأمن الشامل». المجلة العربية للدراسات الأمنية والتدريب 21 (42).

4. رستم، هشام. (2009). «جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة». مجلة الدراسات القانونية (17).

5. عبد الصادق، عادل. (2012). «القوة الإلكترونية: اسلحة الانتشار الشامل في عصر الفضاء الإلكتروني». مجلة السياسة الدولية (188)

6. الفتلاوي، حمد عبيس نعمة. (2016). «الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر». مجلة المحقق الحلي للعلوم القانونية والسياسية 8 (4)

7. كلارك، ريتشارد، وكنيك، روبرت. (2012). *حرب الفضاء الإلكتروني: الخطر القادم على الأمن القومي وسبل مواجهته*. أبو ظبي، الإمارات العربية المتحدة: مركز الإمارات لدراسة السياسات.

8. كلاع، شريفة. (2022). «الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني». مجلة الحقوق والعلوم الانسانية 15 (1).

9. لين، هربرت. (2012). «النزاع السيبراني في القانون الدولي الإنساني». المجلة الدولية للصليب الأحمر 94 (886)

رابعاً: القوانين

1. الدستور العراقي الدائم لسنة ٢٠٠٥

2. قانون جهاز مكافحة الارهاب لسنة ٢٠٠٨

3. مشروع قانون جرائم المعلومات لسنة ٢٠١٨

خامساً: المواقع الالكترونية

1. خريسان، باسم علي. (2020، فبراير 28). «العراق وتحدي الفضاء السيبراني: قراءة في مؤشر الامن السيبراني العالمي». صحيفة كتابات. https://kitabat.com/2020/02/28

2. الربيعة، صالح بن علي بن عبد الرحمن. (د.ت). «الأمن الرقمي وحماية المستخدم من مخاطر الانترنت» على الرابط. https://edu.moe.gov.sa/jeddah

3. الزبيدي، زاهر. (2018). «تهديدات افتراضية للأمن السيبراني العراقي». موقع شبكة النبأ المعلوماتية. https://annabaa.org/arabic/informatics/17379

4. صباح، محمد. (2020). «قانون جرائم المعلوماتية: 21 مادة سالبة للحرية و63 عقوبة حبس وغرامة». موقع صحيفة المدى. https://almadapaper.net/view.php?cat=231679

5. العبودي، علي عبد الرحيم. (2019). «هاجس الحروب السهيبرانية وتداياتها على الأمن والسلم الدوليين». المجلة العلمية الأكاديمية العراقية، 57، 89-118. https://cutt.ly/XkokTen

6. العوادي، هاشم. (2020، يناير 14). «حماية الأمن السيبراني العراقي الاستراتيجية المفقودة». صحيفة كتابات. https://kitabat.com/2020/01/14

7. الكبيسي، صفاء. (2022). «محاولات جديدة لتشريع قانون جرائم المعلوماتية تثير جدلاً في العراق». موقع صحيفة العربي الجديد. https://www.alaraby.co.uk/entertainment_media

8. مهدي، سيماء علي. (2022). «جريمة النشر الالكتروني وفق القانون العراقي». مؤسسة الحوار المتمدن. تمت المراجعة: - 31/1/2022 على الرابط: https://www.ahewar.org/debat/show.art.asp?aid=745498