اشكالية الامن السيبراني العراقي بين التهديدات السيبرانية والتقنين المقيد للحريات

م.د. احمد عبد الكريم عبد الوهاب م.د. محمود عبد الرحمن خلف

كلية العلوم السياسية بجامعة بغداد كلية العلوم للبنات بجامعة بغداد

يمثلَ

الفضاء السيبراني إشكالية معاصرة للأمن الوطني العراقي ، بما يحمله من تهديدات ومخاطر عدة ، ولكي نحافظ على الفضاء السيبراني العراقي أمناً من المخاطر و التهديدات ينبغي توفر حاضن تنظيمي وتشريعي ، بيد ان هذا الحاضن التشريعي والتنظيمي سوف يصطدم بحاجز الحفاظ على الحريات العامة التي ينص عليها الدستور العراقي ، وهذا ما تناولته إشكالية الدراسة في ثلاثة محاور على التوالي ، الأول أختص بتوضيح مفهوم الأمن السيبراني ، اما الثاني تناول توضيح التهديدات و المخاطر التي تحيط بالفضاء السيبراني العراقي ، اما الثالث وضّح أبعاد مقترح قانون الجرائم المعلوماتية العراقي.

Abstract

The problem of Iraqi cybersecurity between cyber threats and restrictive codification of freedoms

Cyberspace is a contemporary problem for the Iraqi national security, with many threats and dangers. In order to keep the Iraqi cyberspace safe from threats and threats, there must be a regulatory and legislative incubator. The first is to clarify the concept of cybersecurity, the second is to clarify the threats and dangers that surround the Iraqi cyberspace, and the third is to clarify the dimensions of the proposed crime law Iraqi Information.

الكلمات المفتاحية: السيبرانية–الامن الوطني–التهديد–المخاطر–الحريات العامة–التطبيق

المقدمة

لا مراء ان الامن الركيزة الاساسية للمجتمع، وقد تحول الامن، مع بروز مجتمع المعلومات، والفضاء السيبراني، الى واحد من قطاعات الخدمات، التي تشكل قيمة مضافة، ودعامة اساسية، لانشطةالفاعلين الدوليين وغير الدوليين على السواء، كما هو الحال، مع التطبيقات الخاصة بالحكومة الالكترونية، والصحة الالكترونية، والتعليم عن بعد، والاستعلام، والتجارة الالكترونية، وغيرها الكثير. الا ان الوجوه المتعددة للامنالسيبراني، ومضاعفاتها الخطيرة التي لا تقف عند حدود الاساءة الى الافراد، والمؤسسات، بل تتعداها الى تعريض سلامة الدول والحكومات، تزيد مهمة القائمين على الموضوع تعقيداً وصعوبة، وتستدعي مقاربة، شاملة، ومتكاملة، لجميع التهديدات، التي يطرحها الفضاء السيبراني، بحيث تأتي الردود، والحلول المقترحة، ناجعة وفاعلةفي تحقيق الامن، وبناء الثقة في الفضاء السيبراني، من أساسيات تسخير تقنيات المعلومات والاتصالات، في مجالات التنمية الشاملة خدمةً للمجتمعات الانسانية .

: أهمية البحث

في ظل الأوضاع الأمنية غير المستقرة التي يشهدها العراق و منطقة الشرق الأوسط عموماً ، ومع تسارع التطورات التكنولوجية الكبيرة التي يشهدها عالم اليوم ، لم تعد سياسات الدفاع و الأمن العراقية مقتصرة على مكافحة الأرهاب وحماية سيادته والمحافظة على أستقراره ووحدته من خلال الاعتماد على الطرق التقليدية فقط، بل تجاوزتها لتشمل حماية أمن المجتمع و الدولة من التهديدات التي أفرزتها الثورة التكنولوجية المعلوماتية المعاصرة ، وذلك يتطلب تحقيق الأمن السيبرانيبأعتباره من أولويات السياسة الدفاعية العراقية .

: إشكالية البحث

يثير البحث سؤال : كيف نوفر للأمن السيبراني العراقي ألية تشريعية وتنظيمية تحصنه في ظل التطور التكنولوجي وما يرافق ذلك من تهديدات ومخاطر على الأمن الوطني العراقي ويجعله عرضة للأختراق ، دون ان تكون هذه الألية التشريعية و التنظيمية أداة لانتهاك الخصوصية وتقيد للحريات العامة .

: فرضية البحث

ان الامن السيبراني العراقي تحيط به التهديدات و المخاطر و التجاوزات بحكم تمتعه بالحرية شبه مطلقة ، و ان محاولة السلطات في العراق الحد من هذه التهديدات و المخاطر و التجاوزات سوف تصطدم بحدود الحريات العامة التي ينص عليها الدستور .

: منهجية البحث

بغية الوصول الى فرضية البحث اعتمدنا منهج التحليل الوصفي للوصول الى النتائج التي يتوخاها البحث .

: هيكلية البحث

لا بد من التوقف بدايةً ، عند ماهية الامن السيبراني، والأخطار السيبرانية، لنستعرض بعدها أبعاد هذا الامن،، وما يرتبط به من تهديدات، مع التركيز على الاطارين التشريعي والتنظيمي في العراق، والصعوبات الاكثر بروزاً، لنصل الى أساسيات إشكالية الدراسة .

: وقد قسم البحث على ثلاثة محاور

المحور الاول : تعريف الامن السيبراني

المحور الثاني: التهديدات و المخاطر السيبرانية

"المحور الثالث: مشروع قانون "جرائم المعلوماتية

المحور الاول : تعريف الامن السيبراني

التعريف لغةً : الأمن السيبراني لابد لنا ان نتعرف على اصل ومعنى كلمة سيبراني ، الكلمة تعتبر ترجمة حرفية لكلمة والتي **Cybernetics** والمشتقة من كلمة **Cyber** استخدمت في الماضي للدلالة كيفية تواصل الآلات والكائنات الحية مع بعض وتحكمها، ومن تلك الكلمة نشأت مصطلحات كثيرة استخدمت في قصص وأفلام أو الفضاء **Cyberspace** الخيال العلمي مثل مصطلح السيبراني والذي يستخدم عادةً للإشارة إلى الإنترنت (وشبكات الاتصالات وكأنها فضاء وهمي أو افتراضي .(1

التعريف إصطلاحاً : الأمن السيبراني

فهو كما عرفه الاتحاد الدولي(Cybersecurity) للاتصالات : " عبارة عن مجموعة الوسائل التقنية والتنظيمية والادارية التي يتم استخدامها لمنع الاستخدام غير المصرح به ، وسوء الاستغلال ، واستعادة المعلومات الإلكترونية ، ونظم الاتصالات والمعلومات التي تحتويها،وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات ، وتعزيز حماية وسرية وخصوصية البيانات الشخصية ، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني".(2)

ويعرف الامن السيبراني بكونه " مجموعة من المهمات، مثل تجميع وسائل، وسياسات، واجراءات امنية، ومبادىء توجيهية، ومقاربات لادارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين " .(3)

بينما يعرف الامن السيبراني في موضع أخر كونه " هو الركن الرئيس لأي نشاط الإلكتروني ، و ينبغي النظر إليه كخدمة تمكن من خلق خدمات أخرى مثل الحكومة الالكترونية ، والصحة الالكترونية ، و التعليم الالكتروني ، و تولد لهذه الخدمات قيمة .(4)

و قد قدمت وزارة الدفاع في الولايات المتحدة الأمريكية تعريفاً دقيقاً لمصطلح الأمن السيبراني ، إذ عدتّه : " جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها (الإلكترونية والمادية)، من مختلف

الجرائم ، الهجمات ، التخريب ، التجسس ، و الحوادث.(5)

في حين عدّ الاتحاد الاوروبي الأمن السيبراني بأنه : " قدرة النظام المعلوماتي على مقاومة محاولات الأختراق أو الحوادث غير المتوقعة ، التي تستهدف البيانات .(6)

و يبدو ان الأمن السيبراني هو سلاح استراتيجيفي متناول يد الافراد و الحكومات لا سيما ان الحرب السيبرانية اصبحت جزء لا يتجزأ من الحروب و الهجمات الحديثة بين الدول .

وبناءً على ما تقدم، يمكن تعريف الامن السيبراني، انطلاقاً من أهدافه، بانه النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن امكانات الحد من الخسائر والاضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع الى ما كان عليه، باسرع وقت ممكن، بحيث لا تتوقف عجلة الانتاج، وبحيث، لا تتحول الاضرار الى خسائر دائمة.

ان الحصول على قدر كافٍ من (أمن المعلومات) لمواجهة مخاطر التكنولوجيا و المعلومات أمر ضروري للأداء السليم للحكومات و المنظمات ، كما ان الاستخدام الشائع و العريض للتكنولوجيات الرقمية يسير يداً بيد مع الاعتماد المتزايد على تلك التكنولوجيات و الاعتماد المتبادل من جانب البنيات التحتية الحرجة ، و هذا يخلق تعارضاً لا يستهان به في أداء المؤسسات ، وربما أدى الى تعريضها للخطر بل وربما الى تقويض الدول .(7)

والعلاقة بين الامن المعلوماتي والامن السيبراني علاقة الجزء بالكل ، إذ يهتم أمن المعلومات بحماية المعلومات من الوصول غير المصرح به ، المعلومات قد تكون على هيئة وثائق ورقية أو مخزنة في وسائط إلكترونية. ومن هنا يمكن القول بأن تأمين المعلومات بغض النظر عن وسيلة حفظها يدخل في نطاق أمن المعلومات، ولكن لا يمكن أبداً أن نقول بأن أمن المعلومات يشمل الأمن السيبراني، كما لا يمكن أن نقول إن الأمن السيبراني يشمل أمن المعلومات.(8)

اما الأمن السيبراني يشمل أمن المعلومات التي يتم نقلها أو تخزينها أو معالجتها في أنظمة الاتصالات وتقنية المعلومات، هذا صحيح، لكنه أيضاً يشمل الحفاظ على توافر وسلامة الخدمات التي يتم تقديمها عبر الفضاء السيبراني كالطاقة الكهربائية ووسائل الاتصالات، وبالتالي لا يصح أن نقول إن أمن المعلومات يشمل الأمن السيبراني، لأن أمن المعلومات يهتم بحماية المعلومات ولا يكترث بمدى سلامة وتوافر الخدمات الإلكترونية. كما لا يصح أن نقول إن الأمن السيبراني يشمل أمن المعلومات لأنه لا علاقة له بأمن المعلومات المدونة على الوثائق الورقية كونها لا تقع في نطاق الفضاء السيبراني.(9)

أذن الأمن السيبراني يشترك – بلا شك– مع أمن المعلومات في حماية المعلومات المتداولة عبر الفضاء السيبراني، وهذه المعلومات لا تخلو من ثلاث حالات هي : الحالة الأولى أن تكون المعلومة مخزنة في وسيلة تخزين إلكترونية، وتعتبر في حالة سُبات حتى يتم استدعاؤها للانتقال إلى مكان آخر. الحالة الثانية أن تكون تحت المعالجة في إحدى المعالجات الإلكترونية، أو كما يحلو للبعض تسميتها (العقول الإلكترونية). الحالة الثالثة أن تكون المعلومات في حالة سفر من مكان إلى آخر عبر الفضاء السيبراني الرحيب. حفظ المعلومات في هذه الحالات الثلاث يُعد منطقة مشتركة بين كل من الأمن

السيبراني وأمن المعلومات، وهذه المنطقة المشتركة هي سبب الارتباك في فهم الخط الفاصل بين المفهومين حتى عند بعض المتخصصين. كلا التخصصين يحتاج فهماً عميقاً للمفاهيم التكنولوجية التي بنيت على أساسها أنظمة الاتصالات وتقنية المعلومات من جهة، كما يحتاج إلى معرفة الإجراءات الأمنية المتعلقة بحماية المعلومات المتداولة،ومعرفة المسائل الأمنية والتدريب عليها يمكن أن يحصل عليها الشخص المثابر عبر القراءة والالتحاق بالدورات المتخصصة في مجال الأمن، لكن الجانب الفني يبقى تحدياً كبيراً يصعب الحصول عليه بدون تأسيس (أكاديمي محترف.(10

لاسيما ان العالم أمسى يواجه كم هائل من المحددات الجديدة للأمن العالمي نتيجة الكثير من المتغيرات ، لعل من أهمها ما يتعلق بعملية تزايد ارتباط البنية الكونية للمعلومات بالفضاء السيبراني ، بما يجعلها عرضة للهجمات السيبرانية في ظل اتساع حركة الفاعلين من غير الدول في استعمالها ، ومن أهم خصائص الأمن (السيبراني تتمثل بما يأتي : (11

1_ الأمن السيبراني رافد جديد للأمن القومي

أصبحت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانية تعرض المصالح الاستراتيجية – ذات الطبيعة الإلكترونية – وتحول الفضاء الإلكتروني لوسيط ومصدر لأدوات جديدة للصراع الدولي المتعدد الأطراف من جهة ، و من جهة أخرى ، فرضت تلك التطورات إعادة التفكير في مفهوم الأمن القومي الذي يعنى بحماية قيّم المجتمع الاساسية وابعاد مصادر التهديد عنها .

2_ الأمن السيبراني جزء من الأمن الجماعي

يعنى الأمن السيبراني بعملية وضع المعايير و الاجراءات المتخذة لمنع وصول المعلومات الى أيدي أشخاص غير مخولين ، وجاءت تلك المظاهر لتبرز استخدامات غير سلمية للفضاء السيبراني ، و ما يمثله ذلك من تهديد للأمن السيبراني العالمي من جانب كافة الفاعلين في مجتمع المعلومات العالمي ، على أساس ان أمن الدولة جزء من الأمن الجماعي .

3_ تصاعد البعد الدولي في مواجهة الأخطار السيبرانية

باتت قضية أمن الفضاء السيبراني قضية دولية تتطلبة استراتيجية مرنة تتوأم مع المتغيرات المستمرة ، سواء أكان في الآليات ، أم في التكتيكات الخاصة بالأمن مقابل التطور المستمر في الأخطار، ويرجع ذلك الى الطبيعة المتغيرة للفضاء السيبراني وفقاً للعامل الإنساني .

4_ الأمن السيبراني كقضية عسكرية واستراتيجية

بدايات الانترنت، قد طورت في بيئة عسكرية، بشكل أساسي، لتضاف اليها فيما بعد البيئة الاكاديمية، بما تمثل من أبحاث تخدم تطوير القدرات العسكرية، والانجازات العلمية، التي تحافظ على تفوق بلد على آخر، حيث كان التنافس على أشده، بين الاتحاد السوفياتي، والولايات المتحدة الاميركية، في مجال الوصول الى الفضاء الخارجي، وتطوير الاسلحة النووية. وتتراكم الامثلة التي يمكن سوقها، في هذا المجال، لتوضيح الابعاد العسكرية، للأمن السيبراني، وخطورة الهجمات السيبرانية، حيث يمكن ايراد ما حصل في جورجيا، واستونيا، وكوريا الجنوبية، وايران، كمثال على بعض الهجمات والاختراقات، التي ترجمت ماديا، سواء باندلا ع صراع مسلح لاحق، كذلك الذي وقع، بين روسيا وجورجيا، أوبانقطاع الاتصال

بالانترنت في استونيا، بين الدولة والمواطنين، والتشويش على الادارات الحكومية.

كذلك، ترد هنا، اختراقات أنظمة المنشآت النووية، في ايران، وتحقق امكانات التلاعب بها، مع ما يعنيه هذا من تعرض الامن القومي، للدولة المعنية، ومن تعريض السلام الدولي للاهتزاز. في هذا المجال ايضا، يمكن ايراد، الاختراق الذي حصل في البرازيل، والمملكة المتحدة، للبنية التحتية للطاقة، حيث انقطع التيار الكهربائي، ما طال بآثاره السلبية ملايين الاشخاص، والمؤسسات والمصالح، وما يمكن ان يعني من وصول، الى موارد الطاقة كافة.

5_ تصاعد خطر الفاعلين من غير الدول على الأمن السيبراني

ان تصاعد دور الفاعلين من غير الدول في العلاقات الدولية ما أثر بدوره على سيادة الدول ، لا سيما مع بروز دور الشركات التكنولوجية العابرة للحدود الدولية ، وبروز أخطار القرصنة و الجريمة السيبرانية ، و الجماعات الارهابية ، و قد بدأ يظهر اتجاه التعددية في الحافظ على الأمن بين كل أصحاب المصلحة من الحكومات ، و المجتمع المدني ، و القطاعين الأكاديمي و التقني ، و القطاع الخاص ، ووسائل الاعلام .

وعليه ، أصبح للفضاء السيبراني دور في وجود أهداف ووسائل ومصالح سيبرانية جديدة ، وفي الوقت عينه أتاح القابلية لخطر التعرض للهجوم ، وهو ما أوجد نوعاً جديداً من التهديدات و المخاطر و أحداث أضرار ، دون الحاجة للدخول او الهجوم الطبيعي والمادي لإقليم الدولة (أي تهديد الأمن القومي) ، و بذلك أرتبط الأمن السيبراني بالأمن القومي ، و ذلك لاعتماد الدول على الأنظمة السيبرانية في أغلب منشأتها الحيوية بما يجعل من تلك الأنظمة هدفاً للهجوم ، خاصة ان تلك الأنظمة تحمل طابعاً مدنياً و عسكرياً مزدوجاً .

المحور الثاني: التهديدات و المخاطر السيبرانية

تصدرالتهديدات والأخطار السيبرانية عن أعمال قصدية، مثل الهجوم والاختراق والاعتداء ، وأعمال غير قصدية، كالاهمال، وقلة الوعي والادراك ، ويمكن أجمالها و تنصيفهابما يأتي :

1_ الهجمات السيبرانية Cyber attacks

و هي بدورها تنقسم الى قسمين بحسب اهدافها :

أ_ الهجمات السيبرانية الدولية : كل ما يعرض الامن القومي، والعسكري، والاقتصادي، والاجتماعي، ويهدد البنية التحتية والحرجة للدول، وأسواق المال والقطاعات المصرفية، والسلم الدولي، والمنشآت النووية، والمؤسسات الصحية، وقطاعات النقل بكل انواعه: البري والبحري والجوي، ورفاه الشعوب.

ب_ الهجمات السيبرانية الشخصية : و تشمل سرقة البيانات الشخصية، وتسريبها، واستخدامها دون اذن، ودون وجه حق، وسرقة الاموال، واختراق انظمة المعلومات، والاعتداء على الملكية الفكرية، والصناعية، والعلامات التجارية. كما تشمل هذه الفئة أيضا: الاحتيال، والبريد غير المرغوب فيه، والجرائم ضد الاطفال، والمحتوى غير المشروع، وغيرها الكثير مما يعتبر جرائم سيبرانية، ضد الاشخاص وضد الاموال.(12)

2_ شبكات التواصل الاجتماعي Social Media))

وتدرج ضمن المخاطر و الاعمال ذات فاعلية مزدوجة ، أي قصدية و غير قصدية ، وقبل التحدث عن نماذج

الاستخدام السيء لشبكات التواصل الاجتماعي وأدوات الإعلام الرقمي ، من المهم ان نوضح كيف غيرت شبكات التواصل الاجتماعي مفاهيم أساسية في صناعة الإعلام حتى أصبحت إحدى أقوى أدوات الضغط السياسي ، كما شكلت أداة مهمة لإحداث تغيرات سياسية عديدة ، أبان ما يسمى بثورات الربيع العربي عام 2011 .

و يكمن تفوق شبكات التواصل الاجتماعي على ما سبقها من وسائل الاعلام التقليدية المركزية القديمة ، و تفوقها على اعلام القنوات الفضائية حيث تعددت مصادر المعلومات و الأخبار ، بيد ان كل المراحل الاعلامية السابقة لم تستطع تهديد و أخطار الأمن القومي كما فعلت شبكات التواصل الاجتماعي،وتكمن الأسباب الرئيسة وراء ذلك في نقطتين أساسيتين و هما كما يأتي :(13)

أ_ إستمرارية الاتصال

ان معدل الوقت الذي يقضيها المستخدم متصلاً بهذه الشبكات ساعات عدة متواصلة ، وفي هذا الصدد فإنه من الواضح حالياً ان معظم المستخدمين يقضون ساعات طويلة يومياً متصلين بشبكات التواصل الاجتماعي بشكل رئيس عبر أجهزة الهواتف المحمولة التي تكاد تلتصق بهم أينما ذهبوا ، وهو ما لم يتوفر في كل ما تقدم من وسائل الإعلام التقليدية ، مثل الراديو ، والتلفاز ، والقنوات الفضائية ، و حتى في المراحل الأولى من استخدام الإنترنيت ما قبل ظهور شبكات التواصل الاجتماعي ، فإمكانية استمرارية الاتصال للمستخدم على مدى الساعة عظمت من قوة وأثر المعلومات المتداولة عبر هذه الشبكات ، مثل الفيسبوك ، وتويتر، ويوتيوب ،فضلاً عن تطبيقات التراسل الفوري مثل ماسنجر فيس ، (Instant Messaging) أيمو ، تليجرام ، واتس أب و غيرها ، و بذلك أصبح الوصول للمستخدم يتم تقريباً في كل وقت و في أي مكان، و هو ما لم يتوفر في كل وسائل الاعلام السابقة .

ب_ المستخدم يصنع الخبر

ان المستخدم لشبكات التواصل الاجتماعي هو من يصنع الخبر ، فكل مستخدم يمكنه ان يطرح ما يشاء من اقتراحات او أراء ، و ينشر أى خبر او يقوم بمشاركة خبر من مصادر مجهولة دون أدنى ضوابط على ما ينشر ، و عدم التحقق من مصدر المعلومات و الأخبار ، وهو ما أسهم بشدة في جعل هذه الشبكات مصدراً رئيس لنشر الأخبار المضللة و الإشاعات الكاذبة ، و هذا الأخير يندرج ضمن قلة الوعي و الادراك .

3_ التجسس الالكتروني

لقد أدركت الحكومات وأجهزة الاستخبارت أهمية شبكات التواصل الاجتماعي ، إذ أمست ميدان جديد لجمع المعلومات وتحليلها ، وقد تم استخدام تطبيقات الذكاء الصناعي و أليات تحليل البيانات الكبيرة (Big Data) لقياس توجهات الرأى العام في دولة ما ، أو تحليل الأوضاع السياسية ، أو أحياناً إدارة المعلومات لإحداث اضطرابات سياسية في دولة ما (كما حدث أبان ما يسمى ثورات الربيع العربي عام 2011) ، أو محاولة تغيير الرأى العام و أعادة توجيه (مثل ما حدث أبان الانتخابات الرئاسية في الولايات المتحدة الامريكية عام 2016) ، وهو ما شكل فضيحة عالمية لتورط الشركة المالكة لموقع التواصل الاجتماعي الفيسبوك في التهاون عن حماية أمن معلومات المستخدمين ، وفقاً لما ذكرته صحيفة النيويورك تايمز الامريكية و صحيفة ذا اوبزرفر البريطانية في 17 أذار

2018 ، اذ تم جمع معلومات عما يقرب 80 مليون مواطن أمريكي ، منالبيانات التي حصلت عليها شركة كامبردج أناليتيكا للاستشارات، وإجراء تحليل سيكولوجية لتوجهاتهم السياسية ، وتمت محاولة التأثير في هؤلاء المستخدمين بنشر أخبار ومعلومات من شأنها دعم موقف الرئيس الأمريكي دونالد ترامب على حساب منافسته (هيلاري كلينتون .(14

3_ الأرهابالسيبراني Cyber terrorism

ويقصد به "هو استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية " (15) ، ويُعرف بكونه"العدوان و التخويف او التهديد مادياً أو معنوياً بإستخدام الوسائل الالكترونية الصادرة من دول او جماعات او افراد على الانسان في دينه ،او نفسه ، او عرضه ،او عقله ، او ماله بغير حق بشتى صنوفه وصور الأفساد في الأرض " (16) و هو يتميز بإستغلال التقدم التكنولوجي بما فيها تكنولوجيا الاتصالات و المعلومات و الشبكة العنكبوتية ، من قبل الجماعات و المنظمات الأرهابية بدوافع سياسية ، من أجل التخطيط لأفعالهم الأرهابية وإعدادها و تنظيمها مع ما يترتب على ذلك من أضرار بالغة في جميع المجالات الاقتصادية والاجتماعية و السياسية و التي قد تصل الى حد تقويض سلطة الدولة ، و تهديد أمنها القومي ، فالأرهاب يستهدف بالعموم ثلاث فئات ، الأولى هم الأنصار او الاتباع الحاليون ،أو المحتملون ، والثانية الرأى العام الدولي ، اما الفئة الثالثة (هي جماهير العدو .(17

لقد وجدت أغلب التنظيمات الأرهابية ضالتها المنشودة في شبكات التواصل الاجتماعي وأعطت الأولوية لها ، وجندت عناصرها للتركيز على هذه الساحة الجديدة للصراع الأيديولوجي بين أفكار هذه التنظيمات من جانب ، و الدولة و مؤسساتها من جانب أخر ، و قد وفرت شبكات التواصل الاجتماعي أدوات عدة و ساعدت هذه التنظيمات على العمل بشكل ميسر ، إذ انها من حيث المبدأ تسمح لأي شخص ان ينتحل أي مسمى و أي صفة ، و اتاحت و Pages الفرصة لإنشاء ما يطلق عليه الصفحات بأنواعها المختلفة ، سواء Groups المجموعات Public أكانت المجموعات العامة المتاحة للجميع ام Closed group ام المجموعات المغلقة group وقد استفادت ، Secret group المجموعات السرية التنظيمات الأرهابية من هذه التقنيات و الصفحات للترويج لأفكارها و التواصل مع مؤيديها أو من تسعى لأجتذابهم ، فضلاً عن تقنية المجموعات السرية لخلق بيئة افتراضية أمنة للتواصل مع أعضائها ، او نقل المهام لهم وعقد اجتماعات افتراضية لأشخاص ربما يكونوا في مدن او بلاد مختلفة (بمعزل عن رقابة ورصد الأجهزة الأمنية .(18

وبذلك أصبحت التنظيمات الأرهابية شبكية وليست هرمية كما في السابق، فيما تُتخذ القرارات في الفضاء السيبراني، لتنفذ الأوامر على أرض الواقع بعد تلقيها عن بعد عبر شبكات التواصل الاجتماعي. والأخطر من ذلك يتمثل في أن الفرد الواحد قد تحول إلى "منظمة إرهابية" او ما يمكن تسميته بالذئاب المنفرد، ما يعني أن انتشار الفكرة عبر الفضاء السيبراني لا يشترط لتطبيقها وجود مجموعة تتبنى هذه الفكرة، بل يكفي فرد واحد لتنفيذها، وهو ما يضعنا

أمام افتراض مفاده أن عددًا من التفجيرات التي تمت في مناطق مختلفة في الدول لا يشترط أن تأتي بناءً على أوامر مركزية من جماعة أرهابية ما، في ظل ما بات يُسمى بـ" بالذئاب المنفردة " في ضوء وجود العديد من المواقع الإلكترونية التي تُديرها عناصر وقيادات الجماعات الأرهابية، والتي توضح محتوياتها الإعلامية كيفية إعداد قنبلة وتلغيم السيارات والمنشآت، كما توضح بعض هذه المواقع الإلكترونية كيفية سرقة الحسابات البنكية، وبطاقات الائتمان، بهدف توفير وتأمين التمويل اللازم للقيام بالعمليات التفجيرية .(19)

لقد قامت التنظيمات الارهابية مثل تنظيم "القاعدة " برفع مستوى انتشاره على الانترنيت وجعل تعليماته حول متى وكيف تنفذ هجماته الأرهابية ، إذ أصدرت جبهة الإعلام الإسلامي العالمية وهي الذراع الإعلامية للتنظيم ، دليلاً على مواقع الشبكات الاجتماعية المختلفة ، قدمت عبره تعليمات باللغة الإنجليزية لصنع قنبلة ، و استمد هذا الدليل من صانع القنابل الإرهابي الشهير (أبوخباب) الذي قتل جراء ضربة صاروخية أمريكية في باكستان ، وهذا الدليل لديه القدرة على توفير المعرفة الكافية للتطرف الذاتي للأفراد والأرهابيين ، بينما أستعان تنظيم "داعش" الإرهابي موقع "تويتر" الذي يُعّد أهم منصات التواصل الاجتماعي التي تستخدم للتفاعل و التنسيق في أثناء العمليات الإرهابية ، إذ يوجد ما يناهز من 46 الى 70 ألف حساب على موقع تويتر نشطة أنشأها مؤيدو "داعش" ، إذ تستخدم كمنبر لتضخيم وانتشار حركته ، وقد ارسلت حسابات "داعش" ما يناهز 200 ألف تغريدة يومياً تحث على الكراهية و التطرف ، و نتيجة هذا الاستخدام المضطرد لموقع تويتر من قبل "داعش" لنشر الدعاية وتجنيد المتابعين له ، قامت شركة "تويتر" و بالتعاون مع مكتب التحقيقات الفدرالي الامريكي في منتصف عام 2015 بإغلاق نحو 125 ألف حساب يمتلكها "داعش" لتشجيع الأعمال الإرهابية التي يقوم بها أو لتهديد الأفراد و الدول .(20)

4_ الطائفية السيبرانية Cyber Sectarianism

التحول الذي حدث في مفهوم الطائفية كان على مستويين:(21)

الاول: على صعيد الابعاد والمساحات الافقية التي يتمدد فيها حيث أخذ ينتشر في البيئات الافتراضية والعوالم الرقمية على شكل منشورات وتعليقات وصورة وفيديوات تعمل على تأجيج هذا النوع الرقمي من الطائفية التي لم تشهدها السنوات السابقة في العراق.

الثاني: على صعيد بيئة انطلاقه، اذا كانت الطائفية، في احدى اوجهها السابقة، تتواجد في المجتمع الواقعي اولا ثم تنعكس، على نحو بسيط، على الفضاء الرقمي .. أما الان فقد اصبحت الطائفية تنطلق من صفحات التواصل الاجتماعي وشبكاتها الاجتماعية، بل قد يبدأ التحريض منها او ان يمارس على هذه الصفحات الطائفية والتحريض باسماء مستعارة بينما هو في مجتمعه وبين اصدقائه لايتحدث على هذ النحو الطائفي والاسلوب المتطرف.

و يمارس هذا النوع من الطائفية نوعان من الناس: (22)

اولا: نوع مكشوف يمارس طائفيته بشكل علني ومفضوح من غير ادنى خوف لبعده عن يد القانون او المجتمع الذي يرضى او يسكت عن تصريحاته .. اذا ما عرف بها

ثانيا: نوع مُقنع يمارس طائفيته الرقمية تحت ستار الاسماء المستعارة، فتراه يردتي الاقنعة ويُخفي مكان سكنه ولايعلن اي تفاصيل تكشف عن هويته .. يتميز اصحاب الطائفية الرقمية، من النوع الثاني، وهم محور حديثي، بعدة خصائل اجبرتنا على استخدام هذا المصطلح وطرحه على هذا الشكل والعنوان، وهذه السمات هي:

أ_ يعيشون في بغداد او في مناطق مختلطة طائفياً.

ب– يمتلكون شهادات جامعية، وبعضهم طلاب جامعة

ج– يختبئون وراء اقنعة عبر اخفاء اسمائهم الحقيقية والاعتماد على اسماء مستعارة.

د– يمارسون عنفاً رمزياً واضحاًعبر تعليقاتهم وماينشروه.

هـ– يمتلكون وحدة ذهنية، تتحكم في سلوكياتهم وتوجههم نحو التمترس خلف ثوب الطائفة.

و– لايخضعون للمنطق والعقلانية في تصرفاتهم وسلوكياتهم ويتحركون بشكل غير واع.

وبناءً على ما تقدم يمكن القول ان مخاطر وسائل التواصل الاجتماعي على أمن المجتمعات إلى الحد الذي قد يصل إلى انتشار العنف الداخلي، من خلال تهديد الانسجام الاجتماعي والثقافي، حيث يمكن عبر وسائل التواصل الاجتماعي نشر ثقافات وتوجهات وأفكار لا تنسجم مع قيم المجتمع، وربما تعارضها كلية، خصوصاً بالنسبة لفئات الشباب وصغار السن الذين قد لا يملكون حصانة كافية ضد التأثر بهذه الأفكار، ما قد ينتج عنه اغترابهم عن المجتمع وتباعد المسافات بينهم وبينه إلى درجة قد تصل حد العداء أو القطيعة، بحكم قدرة مواقع التواصل الاجتماعي على إقامة عالم افتراضي بديل.

الأخطار التقنية السيبرانية _5

Cyber Technical Risks

تتواكب طبيعة التقنيات والاتصالات، مع اخطار خاصة، مرتبطة بهندستها الخاصة، وبالبيئة التي تعمل في اطارها، اي الفضاء السيبراني. واذا كانت التقنية، والهندسة، والرقمنة، تتحكم بتوسع تقنيات المعلومات والاتصالات، وبالولوج الى الفضاء السيبراني، ورسم حدوده، بما جعل البعض يعتبرونها، قادرة على أداء دور القانون، في تنظيم الفضاء السيبراني، وضبط الاعمال المخلة بأمنه، وصولاً الى انكارهم، على المشرع، حق الاضطلاع بمهمة هذا التنظيم. الا ان هذا الامر لا يستقيم، فقد أثبتت هذه التقنية، انها ليست قادرة، على ضبط التصرف الانساني، وتأمين سلامة الافراد، والمؤسسات والدول، التي اصبحت اكثر اعتمادا عليها. فقد دقت اكثر الدول تقدما، ناقوس الخطر، وعلى اكثر من منبر عالمي، للفت الانتباه الى هشاشة الوضع، والى الخلل العضوي الذي يطال البرمجيات والتجهيزات على السواء، والذي يشكل نقاط ضعف، يمكن استغلالها بسهولة من قبل الخبراء في خرق الانظمة المعلوماتية، والى حجم المخاطر الذي يرتبها هذا الامر.(23)

واذا كان صحيحاً ان الحلول التقنية موجودة، فان الصحيح أيضا، انها حلول قاصرة، كونها لا تستطيع مواكبة الدينامية التي توجدها، كما لا تستطيع مواكبة

التحولات المستمرة في طبيعة المخاطر.فهي تتبع ظهور المشكلة، وتشكل ومن ثم ، رداً محدوداً بالزمان والمكان، كما وبمسألة معينة. هذا عدا عن مهارات المتسللين الى الانظمة والمخربين، وتعدد الجهات المعنية بالامنالسيبراني (تقنيين، مستثمرين، عملاء، مهندسين، مطوري برامج وتطبيقات...)، وانعكاس ذلك، تعقيدات على مستوى الرؤية، والفهم الجامع للمخاطر، كما للتدابير المفروض اتخاذها ولا يغفل عن بالنا، حاجة تقنيات الحماية نفسها، الى الحماية.(24)

وبناءً ما تقدم أنفاً، تصدر المخاطر و التهديدات السيبيرانية، ، بشكل أساسي، عن اعمال قصدية، او غير قصدية، وتزيد خطورتها، متى قابلها قلة وعي وادراك، لاساليب وطرق الوقاية.

وعليه، تتطلب مواجهة المخاطر و التهديدات السيبرانية، ايجاد التعريف المناسب، الذي يحدد التصرفات التي يمكن ان تشكل مصادر حتمية للمخاطر والتهديداتالسيبرانية، كتلك المسيئة والمؤذية خصوصاً الأرهابية و الطائفية ، والتي تستتبع بالتالي، تحديد مسؤولية القائمين بها، كما تحديد السلوك الواجب اتباعه، والذي يعني عدم الالتزام به، امتناعاً او اهمالاً، ترتب مسؤولية ، ويستدعي هذا الأمر أيجاد الاطار التشريعي والتنظيمي الحاضن ممثلاً بمشروع قانون "جرائم المعلوماتية" في العراق ، وهذا ما سوف نتناوله بالتفصيل في المحور الثالث من الدراسة .

"المحور الثالث: مشروع قانون "جرائم المعلوماتية

تَعّد جرائم النشر على شبكة المعلومات الالكترونية او ما يصطلح عليها قانوناً بـ (الجرائم المعلوماتية) من الجرائم المستحدثة في الوسط التشريعي والقانوني ، وينبغي على المشرع عند اعداد او صياغة اي تشريع متعلق باحدى هذه الجرائم ان يلتفت الى اختلاف طبيعة هذه الجرائم عن الجرائم التقليدية ، وذلك لتعلقها باساليب مستحدثة ترتبط بالمعالجة الالكترونية للبيانات ، والتعديل عليها ومافي حكم ذلك ، ما يعني ان شبكة المعلومات الالكترونية قد نهضت بمستوى الجرائم التقليدية الى مستوى اخر ، وهذا التطور يتطلب النهوض وتطوير جوانب قانونية اخرى تتعلق بالتحري والاستدلال والضبط ونوع القضاء المختص .

اولاً : ماهية الجريمة المعلوماتية

وبدايةً لابد ان نشير الى انه لايوجد مصطلح قانوني موحد للدلال على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها : فالبعض يطلق عليها جريمة الغش المعلوماتي ، و البعض الأخر يطلق عليها جريمة الاختلاس او الاحتيال المعلوماتي ، واخرون يفضلون تسميتها بالجريمة المعلوماتية .(25)

وهناك البعض يرى ان هذا النوع من الجرائم ناتج عن التقدم التكنولوجي ، ومدى التطور الذي يطرأ عليه ، وهو متجدد بصفة دائمة ومستمرة لاسيما في مجال تكنولوجيا المعلومات ويفضل ان يطلق عليها اصطلاح "جرائم التكنولوجيا الحديثة" فهي جرائم تكنولوجيا بعّدها مرتبطة ارتباطاً وثيقاً بالتكنولوجيا التي تعتمد اساساً على الحواسيب والهواتف المحمولة الذكية وغيرها من أجهزة تقنية قد تظهر في المستقبل، وهي كذلك جرائم حديثة نظراً لحداثتها النسبية من ناحية وارتباطها الوثيق بما قد يظهر من أجهزة حديثة تكون ذات طاقات تخزينية وسرعة فائقة ومرونة في التشغيل .(26)

ويبدو ان اصطلاح "جرائم المعلوماتية" أفضل لانه عام ويشمل كل تقنيات الحاسوب و المحمول و الانترنيت وكل ما يتعلق بالعالم السيبراني ، اذ يشمل التقنيات الحالية والمستقبلية وكلها مستخدمة في التعامل مع المعلومات . وفي اطار تعريف الفقه القانوني للجريمة المعلوماتية نجد الاتجاهات قد تباينات في هذا السياق بين موسع لمفهوم الجريمة المعلوماتية وبين مضيق لمفهومها ، فمن التعريفات المضيقة لمفهوم الجريمة المعلوماتية تعريفها على انها " كل فعل غير مشروع يكون العلم بتكنولوجيا الحواسيب الألية المختلفة بقدر كبير لازماً لارتكابه من ناحية لملاحقته وتحقيقه من ناحية أخرى " (27)

وحسب هذا التعريف يجب ان تتوفر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة بل كذلك لملاحقتها والتحقيق فيها ، وهذا التعريف يضيق بدرجة كبيرة من الجريمة المعلوماتية .

كذلك من التعريفات الضيقة على انها " الفعل غير المشروع الذي يتورط في ارتكابه الحاسوب ، او هي الفعل الاجرامي الذي يستخدم في اقترافه الحاسوب بإعتباره أداة رئيسة " .(28)

وفي المقابل هناك تعريفات توسعت في تعريف الجريمة المعلوماتية في كونها " كل فعل او امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلومات يهدف الى الاعتداء على الأخرين سواء في الاموال او الاشياء المادية و المعنوية " .(29) ، كما تم تعريفها على انها "كل سلوك سلبي يتم بموجبه الاعتداء على البرامج او المعلومات للأخرين للاستفادة منها في اي صورة كانت".(30)

وقد ذهبت مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية الى تعريف الجريمة المعلوماتية انها :" كل سلوك غير مشروع او غير اخلاقي او غير مصرح به يتعلق بالمعالجة الألية للبيانات او بنقلها ".(31)

وفي تقرير الجرائم المتعلقة بالحاسوب ، أقر المجلس الاوروبي بقيام المخالفة (الجريمة) في "كل حال يتم فيها تغيير معطيات او بيانات او برامج الحاسوب او محوها او كتابتها او اي تدخل أخر في مجال انجاز البيانات او معالجتها ، وتبعاً لذلك تسببت في ضرر اقتصادي او فقد حيازة ملكية شخص أخر ، او بقصد الحصول على كسب اقتصادي غير مشروع له او لشخص أخر".(32)

اما مؤتمر الامم المتحدة العاشر لمنع الجريمة و معاقبة المجرمين فقد تبنى التعريف الآتي للجريمة المعلوماتية بكونها " اية جريمة يمكن ارتكابها بواسطة نظام حاسوبي او شبكة حاسوبية ، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكبها في البيئة الالكترونية" .(33)

ويبدو التعريف الاخير اكثر شمولاً ، اذ حاول الاحاطة قدر الامكان بجميع أشكال الجريمة المعلوماتية سواء التي قد تقع بواسطة النظام المعلوماتي او داخل النظام على المعطيات و البرامج والمعلومات ، كما شمل التعريف جميع الجرائم التي من الممكن ان تقع في البيئة الالكترونية ، إذ لم يركز فاعل الجريمة و مقدراته التقنية، ولا على وسيلة ارتكاب الجريمة او على الغاية والنتيجة التي تسعى لها الجريمة المعلوماتية ، بل انه حاول عدم حصر الجريمة المعلوماتية في نطاق ضيق يتيح المجال لإفلات العديد من صور هذه الجريمة من دائرة العقاب .

"ثانياً : التشريع العراقي لقانون "جرائم المعلوماتية

أعدت الحكومة العراقية مشروع قانون جرائم المعلوماتية وتم احالته الى مجلس النواب عام 2011 وتمت قراءته قراءة اولى في المجلس ولازال قيد التشريع ، ويتضمن مشروع هذا القانون (31) مادة موزعه على اربع فصول حيث تضمن الفصل الاول التعاريف والاهداف والفصل الثاني الاحكام العقابية والفصل الثالث أجراءات جمع الأدلة والتحقيق والمحاكمة والفصل الرابع احكام عامة وختامية بالأضافة الى الاسباب الموجبة، وقد انهى البرلمان قراءته الاولى في جلسته الـ 25 يوم 12\1\2019 (تمهيداً للقراءة الثانية من أجل التصويت عليه.(34

وقد عرف المشرع العراقي الجريمة المعلوماتية على انها " هي نشاط اجرامي ايجابي او سلبي تستخدم فيه تقنية متطورة تكنولوجيا بطريقة مباشرة او غير مباشرة كوسيلة او كهدف لتنفيذ الفعل الاجرامي العمدي في البيئة المعلوماتية (.)35

وقد اشار مشروع القانون في فصل الاحكام العقابية في (مادتين فقط) الى مواد سوء استخدام شبكة الانترنت (لاغراض السب والقذف والتشهير وهما:(36

المادة 21

ثالثاً . يعاقب بالحبس مدة لاتقل عن سنة وبغرامة لاتقل عن (2000000) مليوني دينار ولاتزيد على (5000000) خمسة مليون دينار كل من اعتدى على اي من المبادئ او القيم الدينية او الاخلاقية او الاسرية او الاجتماعية او حرمة الحياة الخاصة عن طريق شبكة المعلومات او اجهزة الحاسوب باي شكل من الاشكال .

المادة 22

ثالثا . يعاقب بالحبس مدة لاتزيد على (2) سنتين وبغرامة لاتقل عن (3000000) ثلاثة ملايين دينار ولاتزيد على (5000000) خمسة ملايين دينار او باحدى هاتين العقوبتين كل من استخدم اجهزة الحاسوب وشبكة المعلومات في نسبه للغير عبارات او صور او اصوات اوأية وسيلة أخرى تنطوي على القذف و السب.

ملاحظات و إنتقادتعلى هاتين المادتين وهي كما يأتي:

1 . ان مشروع القانون لم يولي لجرائم الاداب اهمية بما يتناسب وبقية الجرائم التي شملها القانون كجرائم المال والغش والتلاعب والتزوير المالي والامن الوطني التي ذكرها .

2 . ان مشروع القانون لم ينص صراحة على منع اساءة استخدام الهاتف النقال باعتباره وسيلة من وسائل الاتصال في جرائم المعلوماتية .

3 . ان مشروع القانون لم يُعد الابتزاز الجنسي والتحرش عبر وسائل الاتصال جريمة من جرائم الاداب.

4 . ان مشروع القانون لم يشر الى ان التعبير في شبكة الانترنت يعد وسيلة من وسائل العلانية التي على ضوئها يحكم بتجريم الاعمال كما نص على ذلك قانون العقوبات .

5 . لم ينص مشروع القانون على استحداث دائرة خاصة بمكافحة جرائم المعلوماتية وتكون ضمن هيكلية وزارة

الداخلية كما هو المعمول في عدد من الدول التي شرعت قانون الجرائم المعلوماتية الخاصة بها .

6. لم يشدد مشروع القانون العقوبات الخاصة بجرائم الاداب في حين نجد ان العقوبات الخاصة بالجرائم الاخرى اشد واقوى وهذا يثير التساؤل حول مدى مراعاة البنية الاجتماعية للمجتمع العراقي من قبل المشرع واهتمامه .

7. لم يتطرق مشروع القانون الى العقوبات الخاصة بجرائم الارهاب السيبراني و كذلك لم يذكر اي عقوبات بخصوص المواقع و الصفحات التي تحث على الطائفية .

ثالثاً : ردود الافعال على مشروع قانون الجرائم المعلوماتية العراقي

كانت منظمة حقوق الانسان **Human Rights Watch** أول من ندد و استنكر مشروع هذا القانون إذ وصمه بكونه : قانون سئ الصياغة وعقوباته غاشمه تخرق الحق في إجراءات التقاضي و تنتهك حرية التعبير.(37)

وقد فصلت منظمة حقوق الانسان الفقرات التي تنتهك حرية الافراد ، أذ تقول المادة 21و كذلك المادة 22 ان نطاق تلك المادتين واسع وفضفاض و لاتخضع الى معايير محددة ،وبالسماح للسلطات العراقية بمعاقبة الأفراد بهذه الطريقة ، تبدو أحكام القانون متعارضة مع القانون الدولي والدستور العراقي ، واذا تم تطبيقها فسوف تشكل تقليصاً خطيراً لحق العراقيين في حرية التعبير وتكوين الجمعيات .(38)

كما يرفض تقرير منظمة حقوق الانسان المادة 3 في قانون الجرائم المعلوماتية المقترح ، إذ تنص "على السجن المؤبد و على غرامة تتراوح بين 25000000 الى 5000000 لكل من استخدام أجهزة الحاسوب بأي شكل من الأشكال مع "جهة معادية " ؛ بقصد زعزعة الأمن و النظام العام أو تعريض البلاد للخطر" ، إذ يمكن ان يكون هذا النص القانوني بمثابة الاساس لمحاكمة كل من لديه أي ارتباط مع منظمة او حركة تُعد "معادية" لانها تنتقد الحكومة أو السياسات الحكومية ، ويمكن للمسؤولين في السلطة او الحكومة ان يعتبروا أية منظمة او الاحزاب السياسية المعارضة "معادية" .(39)

ومن جانب أخر ، وجهت الى قانون الجرائم المعلوماتية جملة من الانتقادات او الملاحظات التي لايمكن اهمالها لكونها تحمل طابع تقويمياً ومنها على سبيل المثال لا الحصر كون اغلب العقوبات في القانون المقترح فيها قسوة واضحة في أغلب العقوبات المقترحة،فلو طبقت فقرات هذا القانون على مستخدمي البيئة الالكترونية المعلوماتية الواسعة فان غالبية الشعب العراقي سوف تكون في موضع الاتهام وفي مقدمتهم الطبقة السياسية الحاكمة، وقد لا تكفي السجون لاستيعاب كل من تشملهم العقوبات القاسية في هذا القانون، وكما هناك نظرة ضيقة في إطار القانون لأنه يقتصر على ما يسميه(جرائم الحاسوب) في حين أن البيئة الالكترونية المعلوماتية أوسع من ذلك بكثير .(40)

كما تضمّن الفصل الثاني من مشروع القانون المقترح أحكاماً عقابية قاسية قد لا يوجد لها مثيل في تشريعات الدول الأخرى، فقد تكررت عقوبة (السجن المؤبد) في المواد 3 و 4 و 5 و 6 وتشمل عدداً كبيراً من الجرائم التي لا تقتضي في أغلبها هذا النوع من العقوبة القصوى، ومثال على ذلك الفقرة ثالثا من المادة 6:" نشر أو إذاعة وقائع كاذبة أو مضللة بقصد إضعاف الثقة بالنظام المالي الالكتروني أوالأوراق التجارية والمالية الالكترونية وما في

حكمها أو الإضرار بالاقتصاد الوطني والثقة المالية للدولة . ((41

كذلك المادتان 7–8 تنصان على عقوبة (السجن المؤقت) مع غرامات مالية وذلك دون تحديد مدة(السجن المؤقت)،أما المواد من 9 الى 23 فتتضمن عقوبة الحبس أو السجن لمدد متفاوتة تتراوح مابين عام واحد الى عشرة أعوام، إلى جانب غرامات مالية كبيرة ،أما الجرائم التي تشملها هذه العقوبات فهي متعددة ومتنوعة، ومثال على ذلك الفقرة ثانياً من المادة 18 التي جاء فيها:(يعاقب بالحبس مدة لا تزيد على 3 سنوات وبغرامة لا تقل عن مليوني دينار ولا تزيد عن 3 ملايين دينار كل من استخدم أجهزة الحاسوب وشبكة المعلومات و انتحل صفة او أسماً (ليس له بقصد التضليل أو الغش) .(42

ولسنا بصدد تفصيل جميع مواد القانون المقترح او نقدها وتقويمها ، نقول يجب أن تخضع مسودة قانون جرائم المعلوماتية العراقي للمراجعة من أجل إبراز المبدأ القائل بأن العبء يقع دوماً على عاتق الدولة لإظهار أن الحد من الحريات يأتي دفاعاً عن الشعب تجاه خطر حقيقي محدق ومحتمل ،وإن فرصة المراجعة موجودة بما أن مسودة القانون تنتظر القراءة النهائية لها في مجلس النواب العراقي ، إما إن لم تتم مراجعتها، فسيصبح هذا القانون حلقة أخرى من سلسلة القوانين الضعيفة التي تحتوي على العديد من الفقرات غير الديمقراطية الموروثة من العهود السابقة في العراق، وقابلة للاستخدام في السنوات القادمة في البلاد بالرغم من أنها غير متوائمة مع معظم الالتزامات القانونية الأساسية التي التزم بها العراق بموجب دستوره الحالي والتزاماته الدولية.

الخاتمة و الإستنتاجات

يفتقر العراق الى الخبرات التراكمية ضمن مجال الفضاء السيبراني ، بحكم انه ما يزال في جدته او حداثته في هذا المجال ،الأمر الذي يجعل عملية الحفاظ على أمنه السيبراني من التهديدات و المخاطر أمراً صعباً او شائكاً و إشكالياً ، وهذا مدعاة الى ضرورة التعاون الوثيق بين القطاع العام و الخاص وكافة منظمات المجتمع المدني ، من أجل التوصل الى نشر ثقافة احترام القوانين في الفضاء السيبراني ، و في الوقت عينه الحفاظ على الحقوق و الحريات العامة ، فضلاً عن ان البيئة التشريعية والتنظيمية في العراق مازالت في بواكير أعمالها من أجل تنظيم الفضاء السيبراني العراقي ، ورغم ان العراق عضواً في الاتحاد الدولي للإتصالات ، و كذلك هو عضواً في الشراكة الدولية المتعددة الأطراف لمكافحة السيبرانية (امباكت) ، الا ان الانضمام الى الجهود الدولية، بحاجة الى دينامية اكثر فعالية، سواء أكان عبر انضمام الى الجهود والمنظمات العاملة على برامج امن وسلامة الفضاء السيبيراني، ام عبر الانضمام الى المعاهدات الدولية، المعمول بها حاليا ، إذ ما يزال العراق يحتل مرتبة متأخرة في ترتيب مؤشر الامن السيبراني لعام 2019 بحسب تقرير الاتحاد الدولي للاتصالات التابع للامم المتحدة حيث حل العراق في المركز 107 عالمياً للأمن السيبراني وجاء ترتيبه في المركز 13 عربياً ، وسبقته في هذا الترتيب عدة دول عربية لا يمكن مطلقاً مقارنة موازناتها المالية بالعراق من بينها السودان وفلسطين والأردن ، الأمر الذي يتطلب جملة توصيات للنهوض بواقع الأمن السيبراني العراقي وهي كما يأتي :

التوصيات

1. العملعلىتنسيقوتحديدأولوياتالبحثوالتطويرفيمجالالأمنالسيبراني.
2. العملعلىتوسعةوتعزيزمجتمعالأبحاثفيمجالالأمنالسيبراني .
3. العملعلىتعزيز،تطويروتسويقالملكيةالفكريةوالتكنولوجيةوالابتكاراتمنخلالالبحوثالمركزةوالمتخصصة والتطويرية .
4. العملعلىتغذيةودعمالسوقالمحليوالصناعاتفيمجالالأمنالسيبراني .
5. وضع استراتيجية لنشر الوعي وبنائه، لدى مختلف شرائح المجتمع، سواء منهم المستخدمين العاديين، او المهنيين، او متخذي القرار، والمسؤولين عن سياسات الامن والسلامة.
6. تأمين انسجام الانظمة القانونية،المكافحة للجرائم السيبرانية،بما يمنع من قمع الحريات .
7. وضع اطار تعاون، يضمن تبادل المعلومات، ونقل الممارسات الفضلى، في المجال الامني السيبراني .
8. اتخاذ تدابير تعتمد الامن كعنصر ضروري في الانتاج، لاسيما ما يخص البرامج والاجهزة المستخدمة في تقنيات الاتصال.
9. التزام القرارات الصادرة عن الامم المتحدة وعن القمة العالمية لمجتمع المعلومات بشقيها، والداعية الى نشر ثقافة الامن السيبراني.
10. اعتماد مبادىءأخلاقية للسلوك السيبراني، على مثال أخلاق واصول التعامل القائمة في المجتمع التقليدي، وتكون بمثابة عقد اجتماعي، يؤسس لسلوك، يضمن سلامة الجماعة، وسلامة مواردها.
11. العملعلىاستحداثاختصاصجامعييختصبالأمنالسيبراني **bachelor degree in cyber security** ويكون وفقمعايرخاصة.
12. وضع استراتيجية، وسياسة امنية واضحة وملزمة، لكل المعنيين بصناعة المعلومات، وبادراة وسائل الاتصالات، والبنى التحتية، كما لاولئك المعنيين بصناعة ادوات وبرامج الاتصال، وخزن المعلومات ومعالجتها.
13. إضافةتخصصيعنبالجنائياتالرقمية (**Digital Forensic**) . وطرقالتحقيقوالاثباتفيالقضاياالمتعلقةبالجرائم المعلوماتية
14. اخذ جميع ابعاد الامن السيبراني، بعين الاعتبار، لدى وضع أية استراتيجية او سياسة، بما في ذلك، حاجات المواطنين والمؤسسات، كما حقوقهم وواجباتهم، بحيث تأتي الخطة متكاملة، ومنسجمة مع ما يمكن توقع الالتزام به، من قبل المعنيين، بامن مجتمع المعلومات.
15. إضافةالمناهجوالتخصصاتالتيتعنبالجرائمالمعلوماتيةلطلابكليا تالحقوقوالقضاة.
16. الاقرار بالمسؤولية عن تحقيق الامن السيبراني، كجزء لا يتجزأ من الامن القومي العراقي والوطني.
17. توحيدأنظمةالأمنالسيبرانيعبرجميعمفاصلالدولةالعراقية .

18. انشاء مراكز للسلامة المعلوماتية، ولطوارىء الاتصالات، تتعاون فيما بينها، وفق آلية واضحة وشفافة وفاعلة.

19. العملعلىتقويةوتعزيزالرصدوالتنفيذللمعاييرفيمجالالامنالسيبراني .

20. تدريب وتأهيل وحدات عسكرية وامنية خاصة، يمكنها مراقبة البنى التحتية للاتصالات، بحيث تقوم بتحديد المخاطر المحتملة، وازالتها.

21. وضعإطارمعياريلتقييممخاطرالامنالسيبراني

22. تأهيل الاجهزة القضائية المختصة، والشرطة القضائية، بحيث تتمكن من القيام بواجبها، في مجال ملاحقة ومحاكمة المجرمين السيبرانيين.

23. العملعلىتعزيزوتقويةفريقالاستجابةللحوادثالسيبرانيةالعراقية (CERT).

24. تحويل الامن السيبراني العراقي، الى جزء من خطط التنمية والتطوير كافة.

25. العملعلىوضعآلياتفعالةللإبلاغعنالحوادثالسيبرانية .

26. انشاء هيئات تحكيم وطنيةعراقية،متخصصة في القضايا السيبرانية، وخدمات استشارات، مسبقة ولاحقة لاي نشاط الكتروني، يمكن لمن يرغب، اللجوء اليها.

27. تشجيعالمشاركةالفعالةفيجميعهيئاتالأمنالسيبرانيالدوليةذاتالصلة،والوكالاتالمتعددةالجنسيات .

28. تعزيزالمشاركةالفعالةفيجميعالفعالياتوالمؤتمراتوالمنتدياتالدولية المتعلقةبالأمنالسيبراني

29. تعزيزالموقعالاستراتيجيللعراقفيمجالالأمنالسيبرانيمنعبراستضافة مؤتمراتدوليةدوريةفيمجالالامن السيبراني .

30. التواصلمعمنظمةالاتصالاتالعالمية (ITU) والعملعلىتحديثالملفالمتعلقبالوعيالأمنيالسيبرانيالعراقي .

المصادر :

1_ ينظرالرابط على شبكة الانترنيت:what_is_cyber_scecuryhttps\\www.fadvisor.net\blog\.

2_ عادل عبدالمنعم ، أمن المعلومات والأمن القومي ، مجلة السياسة الدولية، ع 213، 2018 ، ص 202.

3_ منى الأشقر جبور، الأمن السيبراني:التحديات ومستلزمات المواجهة،جامعةالدولالعربية،المركزالعربي للبحوث القانونيةوالقضائية،بيروت، 2012 ، ص 3.

4_ حمدون.أ.توريه ،دليل الأمن السيبراني للبلدان النامية،الاتحادالدوليللأتصالات ،.2006، ص 6

5_ نقلاًعن: محمدمختار، هل يمكن ان تتجنب الدول مخاطر الهجمات الألكترونية، دوريةاتجاهات الأحداث ،مركزالمستقبل للأبحاث والدراسات المتقدمة، ع 56، يناير 2015، ص 11.

6_ المصدرالسابق نفسه ، ص 12.

7_ حمدون.أ.توريه ، مصدرسبق ذكره ، ص 7.

8_ الفرق بين أمن المعلومات و الأمن السيبراني ، مقال على شبكة الانترنيت و على الرابط :
http\\www.alwatan.com.sa\article\37642

9_ الفرق بين أمن المعلومات و الأمن السيبراني ، مقال على شبكة الانترنيت و على الرابط :
http\\www.oolom\6124\

10_ الفرق بين أمن المعلومات و الأمن السيبراني ، مقال على شبكة الانترنيت و على الرابط :

https:\\www.almrsal.com\post\797299

11_ عبدالغفارعفيفي الدويك ، استراتجية الردع السيبراني..التجربة الأمريكية،مجلة السياسة الدولية ، ع 213، 2018، ص 197.

12_ منى الأشقر جبور ، مصدر سبق ذكره ، ص 4.

13_ اسماعيل عبدالفتاح عبدالكافي ، شبكات التواصل والأنترنيت والتأثير على الأمن القومي والاجتماعي ، ط 1، القاهرة ، المكتب العربي للمعارف ، 2016 ، ص 13.

14_ نقلاً عن : عادل عبد المنعم ، مصدرسبق ذكره ، ص 4. وكذلك ينظر : الروابط على شبكة الانترنيت

www.bbc.com\arabic\science-and-tech-4365066

http://arabic.euronews.com\2018\04\05\facebook-says-data-laak-hits-87-million-users-widening-privacy-scandal.

15_ نقلاًعن: الموسوعة الحرة ويكيبديا (الارهاب الالكتروني) و على الرابط الاكتروني :

https:\\ar.wikipedia.org\wiki\

16_ أيسر محمدعطية، دور الأليات الحديثة للحد منالجرائم المستحدثة :الأرهابالألكتروني وطرق مواجهته ، ورقة بحثية مقدمة في الملتقى العلمي : الجرائم المستحدثة في ظل المتغيرات والتحولات الأقليمية و الدولية ، عمان ، 2014 ، ص 9.

17_ عبدالستار بيرقدار ، الارهاب الألكتروني ، وعلى الرابط الالكتروني :

http://www.sotaliraq.com\2019\04\09

18_ عادل عبد المنعم ، مصدر سبق ذكره ، ص 204_205.

19_ حكيم غريب ، مخاطر مواقع التواصل الاجتماعي على الأمن المجتمعي : الرهانات والاستراتجيات ، الندوة النقاشية العلمية الدولية حول : عولمة الاعلام السياسي وتحديات الأمن القومي للدول النامية ، المدرسة الوطنية العليا للعلوم السياسية ، الجزائر ، 2017 ، ص 10.

20_ للمزيد ينظر: نها عبدالمعطي ، منصات الاعلام الاجتماعي وصناعة التطرف والأرهاب .. الواقع و أليات المواجهة ، مجلة السياسة الدولية ، ع 213، 2018، ص 209_210.

21_ مهند حبيب السماوي ، الطائفية الرقمية..قراءة في تحولات مفهوم الطائفية ، صحيفة المثقف ،ع 4719 و على الرابط الالكتروني :

www.almthaqaf.com

22_ المصدر السابق نفسه .

23_5 منى الأشقر جبور ، مصدر سبق ذكره ، ص 6.

24_ المصدر نفسه ، ص 6.

25_ سامي الشوا ، ثورة المعلومات وإنعكاساتها على قانون العقوبات ،ط 1، القاهرة ، دار النهضة العربية ، 1994 ، ص 4.

26_ عفيفي كامل ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ، ط 1، القاهرة ، دار منار ، 2000، ص 20.

27_ نائلة قوره ، جرائم الحاسب الأقتصادية، ط 1، القاهرة ، دار النهضة العربية ، 2004، ص 21.

28_ هلالي عبدالاله أحمد ، التزام الشاهد بالاعلام في الجرائم المعلوماتية ، ط 1، القاهرة ، دار النهضة العربية ، 1997، ص 13.

29_ سامي الشوا ، مصدر سبق ذكره ، ص 5.

30_ محمد حماد الهيتي ، التكنولوجيا الحديثة والقانون الجنائي ، ط 1، عمان، دارالثقافة للنشر،2004،ص 19.

31_ نائلة قوره ، مصدر سبق ذكره ، ص 23.

32_ نقلاًعن : كامل السعيد ، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات ، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ، دار النهضة العربية ، دار النهضة العربية ، 1993، ص 325_324.

33_ أسامة والزغبي المناعة ، صايل جلال والهواوشة ، جرائم الحاسب الألي والانترنيت ، ط 1 ، عمان ، دار وائل للنشر ، 2001 ، ص 78.

34_ ينظر: الرابط على شبكة الانترنيت

baghadtody.news\news\71431

35_ نحو تشريع قانون جرائم المعلومات ، ينظر الرابط على شبكة الانترنيت:

ar.parliament.iq\2018\10\13\2

36_ المصدر السابق نفسه

37_ تقرير منظمة هيومنرايتسووتش وعلى الرابط الالكتروني :

https://www.hrw.org/sites/default/files/reports/iraq0712arForUpload.pdf

38_ المصدر السابق نفسه، ص 3 .

39_ المصدر السابق نفسه ، ص 6 .

40_ قراءة في مشروع قانون جرائم المعلوماتية ، مقال على الرابط الالكتروني :ina.iq\83196

41_ ينظر: مسودة قانون الجرائم المعلوماتية العراقي ،على موقع السومرية نيوز وعلى الرابط الالكتروني :

https://www.alsumaria.tv/mobile/news/257710

42_ المصدر السابق نفسه